# Spartanburg County
# Identity Theft Prevention Policy

## THE PURPOSE

To establish an Identity Theft Prevention Program designed to detect, prevent and mitigate identity theft in connection with sensitive data collected, utilized and stored by Spartanburg County departments. 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:** an account that a department of Spartanburg County 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:** fraud committed or attempted using the identifying information of another person without authority, and includes any terms and definition as defined in SC Code of Laws §16-13-510.

**Personal Identifying Information:** personal information as defined in the SC Code of Laws §16-13-510(d).

**Security Breach:** 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 person.

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

## PROGRAM

Spartanburg County establishes an Identity Theft Prevention Program to detect, prevent and mitigate identity theft. The Program shall include reasonable policies and procedures to:

1. Identity 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 by South Carolina Act 190 of 2008;
6. Ensure the Program is updated periodically to reflect changes in risk to customers.

## ADMINISTRATION

The County Administrator and/or his designee shall be responsible for the development, implementation, oversight and continued administration of the Program. The Program shall ensure that

staff is adequately trained to effectively implement the Program and shall exercise appropriate and effective oversight of service provider arrangements.

## MANAGEMENT AND SECURITY OF PERSONAL IDENTIFYING INFORMATION

The County Administrator and/or his designee shall enact procedures to manage and secure lawfully obtained personal identifying information so that it shall only be disseminated internally for use by employees of the County for legitimate business reasons and externally to the general public only for reasons authorized by state, federal, or local statutes.

Spartanburg County shall disclose a breach in the security data to an entity 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 reasonable 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 the SC Code of Laws §1-11-490(c), or with measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system.

## INDENTIFICATION OF RED FLAGS

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

1. Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;
2. The presentation of suspicious documents;
3. The presentation of suspicious personal identifying information;
4. The unusual use of, or other suspicious activity related to, a covered account; and
5. 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.

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

1. The types of covered accounts offered and maintained;
2. The methods provided to open covered accounts;
3. The methods provided to access covered accounts;
4. It's previous experience with identity theft.

The Program shall incorporate relevant red flags from sources such as:

1. Incidents of identity theft previously experienced;
2. Methods of identity theft that reflect changes in risk; and
3. 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 identify theft;
2. Changes in methods of identity theft;
3. Changes in methods to detect, prevent and mitigate identity theft;
4. Changes in business operations of the County.

## OVERSIGHT OF THE PROGRAM

Oversight of the Program shall include;

1. Assignment of specific responsibility of implementation of the Program;
2. Review of reports prepared by staff regarding compliance with the Program;
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 the County Administrator at least annually on compliance by the County 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 County 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 County engages a service provider to perform an activity in connection with one or more covered accounts.

Approved by County Council 8/17/09