ORIGINAL
STAMPED IN RED

RESOLUTION NO.: R-2009-061

Adopting the City of Columbia's Identity Theft Prevention and Detection and Red Flags Rule Policy Statement

BE IT RESOLVED this 5th day of August, 2009 that the Mayor and City Council of the City of Columbia, South Carolina hereby adopts as official City policy the Identity Theft Prevention and Detection and Red Flag Rules Policy Statement attached hereto. This policy replaces and supersedes all previous identity theft prevention and detection and red flags rule policies of the City or its departments.

Requested by:

Customer Services

Mayor

Approved by:

Interim City Manager

Approved as to form:

City Attorney

ATTEST:

Erika D. Salley
City Clerk

Introduced: 8/5/2009
Final Reading: 8/5/2009

CITY OF COLUMBIA IDENTITY THEFT PREVENTION AND DETECTION AND RED FLAGS RULE POLICY STATEMENT

It is the policy of The City of Columbia to follow all federal and state laws and reporting requirements regarding identity theft. Specifically, this policy outlines how the City of Columbia will (1) identify, (2) detect and (3) respond to "red flags" by its various Departments which fall within the areas governed by the new regulations. A "red flag" as defined by this policy includes a pattern, practice, or specific account or record activity that indicates possible identity theft.

It is the policy of the City of Columbia that this Identity Theft Prevention and Detection and Red Flags Rule compliance program is effective immediately upon issuance by the City Manager, and that the policy is reviewed and approved no less than annually.

It is the policy of The City of Columbia that its business associates contracting with a Department of the City of Columbia which is subject to this policy must be contractually bound to protect sensitive customer information to the same degree as set forth in this policy. It is also the policy of The City of Columbia that business associates who violate their agreement will be dealt with first by an attempt to correct the problem, and if that fails by termination of the agreement and discontinuation of services by the business associate.

It is the policy of the City of Columbia that all members of our workforce within a Department which is subject to this policy have been trained on the policies and procedures governing compliance with the Red Flags Rule. It is also the policy of The City of Columbia that new members of our workforce receive training on these matters within a reasonable time after they have joined the workforce. It is the policy of The City of Columbia to provide training should any policy or procedure related to the Red Flags Rule materially change. This training will be provided within a reasonable time after the policy or procedure materially changes. Furthermore, it is the policy of The City of Columbia that training will be documented, indicating participants, date and subject matter.

The following Departments fall within the guidelines established by this Policy:

Department of Engineering and Utilities, Water Customer Service

I. Red Flag procedures.

The City of Columbia Departments which fall under the policy requirements will be alert for discrepancies in documents and customer information that suggest risk of identity theft or fraud. The City of Columbia will verify customer identity, address and insurance coverage at the time of customer interaction concerning new accounts and/or existing accounts.
Procedure:

1. When an existing customer calls or physically comes to a Department to request information, the customer will be asked to verify proper identification of the customer by use of one or more of the following procedures:

- Driver's license or other photo ID;
- Utility bills or other correspondence showing current residence if the photo ID does not show the customer's current address;
- If contacted by phone, reference to challenge questions to verify proper identification derived from customer's credit report, credit identification service, established upon opening the account, or other information source;
- Verify the password or pass-phrase established in opening the account, if applicable.

2. When a new account is established for a customer, the customer will be asked to verify proper identification of the customer in person by use of one or more of the following procedures:

- Driver's license or other photo ID;
- Utility bills or other correspondence showing current residence if the photo ID does not show the customer's current address;

3. If unusual circumstances which would prevent an in person presentation of the documentation by the customer required to open a new account, such circumstances being documented by the Department, additional safeguards are to be used to verify proper identification of the customer by reference to challenge questions to verify proper identification derived from customer's credit report, credit identification service, or other information source.

4. Upon opening a new account or establishing access via telephone or other remote method, such as internet, the customer may, as directed by the Department, establish a password or pass-phrase to assist with verifying customer identity and authorization to obtain information related to customer's account within the following parameters.

- A social security number may not be used;
- The customer submits a driver's license or other identifying information that appears to be altered or forged;
- Information on one form of identification the customer submitted is inconsistent with information on another form of identification or with information already in the practice's records;
- An address or telephone number is discovered to be incorrect, non-existent or fictitious;
- The customer fails to provide identifying information or documents;
- The customer's signature does not match a signature of record with the Department;

- The identifying information the customer provided is the same as identifying information in the practice's records provided by another individual, or the identifying number is invalid.

5. In order to further prevent the likelihood of Identity Theft occurring with respect to City of Columbia accounts, the Departments shall take the following steps with respect to its internal operating procedures to protect customer identifying information:

- Secure the District website or provide clear notice that the website is not secure;
- Undertake complete and secure destruction of paper documents and computer files containing customer information as dictated by the City of Columbia's documentation retention policy and procedures;
- Make office computers password protected;
- Keep offices clear of papers containing customer identifying information;
- Request only the last 4 digits of social security numbers (if any);
- Maintain computer virus protection up to date; and
- Require and keep only the kinds of customer information that are necessary for District purposes;
- Redact, remove and/or replace with appropriate typographical characters at least one-half (1/2) of any uniquely personal identifying information such as credit card numbers, social security numbers, driver's license numbers, or other similar information from receipts, bills, invoices, and other material released to the United States Postal Service for delivery or for print-out and release to customer so as to obscure the complete identity or nature of such information. Best practice requires no more than four digits of a social security number be shown or used for purposes related to customer's account and that the majority of any credit card number be replaced with typographical characters.

6. Departments should be alert for the possibility of identity theft in the following situations:
- The photograph on a driver's license or other photo ID submitted by the customer does not resemble the customer;
- The customer submits a driver's license or other identifying information that appears to be altered or forged;
- Information on one form of identification the customer submitted is inconsistent with information on another form of identification or with information already in the practice's records;
- An address or telephone number is discovered to be incorrect, non-existent or fictitious;
- The customer fails to provide identifying information or documents;
- The customer's signature does not match a signature of record with the Department;
- The identifying information the customer provided is the same as identifying information in the practice's records provided by another individual, or the identifying number is invalid.

II. Identifying and Detecting Red Flags

In the course of dealings with customers, the City of Columbia may encounter inconsistent or suspicious documents, information or activity that may signal identity theft. The City of Columbia identifies the following as potential red flags, and this policy includes procedures describing how to detect and respond to these red flags below:

1. A complaint or question from a customer based on the customer's receipt of:
- A bill for another individual;
- A bill for a product or service that the customer denies receiving;
- A bill for a service not offered or provided by the City of Columbia; or
- A notice of refund or overcharge not documented by the City of Columbia.

2. A complaint or question from a customer about the receipt of a collection notice from a bill collector.
3. A complaint or question from a customer about information added to a credit report by the City of Columbia not documented within the system.
4. A dispute of a bill by a customer who claims to be the victim of any type of identity theft.
5. A notice or inquiry from a law enforcement agency.

III. Responding to Red Flags

If an employee detects fraudulent activity or if a customer claims to be a victim of identity theft, the City of Columbia will respond to and investigate the situation.

If potentially fraudulent activity (a red flag) is detected by an employee of the City of Columbia, the following responses shall be undertaken:

1. The employee should gather all documentation and report the incident to his or her immediate supervisor or designated compliance officer/privacy official, if applicable.

2. A Department Supervisor, or other designated compliance officer/privacy official, if applicable, will determine whether the activity is fraudulent or authentic.

3. If the activity is determined to be fraudulent, then the City of Columbia should take immediate action. Actions may include:
- Cancel the transaction;
- Notify appropriate law enforcement;
- Notify the affected customer;
- Notify City of Columbia's Legal Department; and
- Assess impact to the specific account and the Department's operation.

If a customer claims to be a victim of identity theft, the following responses shall be undertaken:

1. The customer should be encouraged to file a police report for identity theft if he/she has not done so already.
2. The customer should be encouraged to complete the ID Theft Affidavit developed by the FTC, along with supporting documentation.
3. The City of Columbia will compare the customer's documentation with personal information in its records.
4. If following investigation, it appears that the customer has been a victim of identity theft, the City of Columbia will promptly consider what further act/notifications may be needed under the circumstances, including reporting the action to the City of Columbia's Legal Department.
5. If inaccuracies due to identity theft exist in Department's records on a customer, a notation should be made in the record to indicate identity theft.
6. The Department will determine whether any other records and/or ancillary service providers are linked to inaccurate information. Any additional files containing information relevant to identity theft will be removed and appropriate action taken. The customer is responsible for contacting ancillary service providers.
7. If following investigation, it does not appear that the customer has been a victim of identity theft, the City of Columbia will take whatever action it deems appropriate.