Red Flag Rule

City of Columbia Identity Theft Prevention Program

Effective December, 2010

City Council Adopted and Effective Date: _______________

This document is intended to give guidance to the City in their understanding of the FTC Red Flag Rule. It is not intended to be used in place of compliance, in whole or any part, of the FTC Rule.
08/02/10 Final
11/10/10 Reviewed/Updated

Table of Contents

INTRODUCTION

The City of Columbia (the “City”) has developed this Identity Theft Prevention Program ("Program") pursuant to the Federal Trade Commission's (“FTC”) Red Flag Rule, which implements Section 114 of the Fair and Accurate Credit Transaction Act of 2003, pursuant to 16 C.F.R. §681.2. This Program is designed to detect, prevent and mitigate identity theft not only in connection with the opening and maintenance of City utility accounts but other city accounts, applications, registrations or other transactions, referred to as “Record” or “Records” throughout this Program, where identity theft might occur.

Why did FTC make this rule?
The intent is to protect consumers from identity theft. It is targeted at entities that **obtain** and **hold** consumer identification such as billing addresses, Social Security Numbers, dates of birth, passports or immigration documents, or other information.

Who must comply?
Entities such as Columbia that obtain and hold identification often targeted by identity thieves must comply.

What is a “Red Flag?”
A “Red Flag” is a term the FTC has coined to identify possible identity theft. It is a pattern or particular specific activity that indicates the possible risk of identity theft. The FTC has identified thirty-one “Red Flags” that entities, especially utilities, should watch for. Such entities are required to have a written plan to help employees identify these “Red Flags” and how to respond when a possible identity theft has occurred.

How does Columbia have to comply with this rule?
We have a duty to:

1. Identity Red Flags
2. Detect Red Flags; and
3. Respond to Red Flags

Who within City operations has to comply with the rule?
All City Departments which obtain and hold any of the consumer identification mentioned above must comply with the rule.

For purposes of this Program, "Identity Theft" is considered to be "fraud committed using the identifying information of another person." The Program "Record” is defined as:

1. A continuing relationship the City has with an individual through a Record the City offers or maintains primarily for personal, family or household purposes, that involves multiple payments or transactions; and
2. Any other account, registration, application or record the City offers or maintains for which there is a reasonable foreseeable risk to customers or to the safety and soundness of the City from Identify Theft

This Program was developed with oversight and approval of the Columbia City Council. After consideration of the size and complexity of the City's operations and various systems, and the nature and scope of these activities, the Columbia City Council determined that this Program was appropriate for the City and therefore approved this Program on December 15, 2008.

The Red Flag Rule-City of Columbia Identity Theft Prevention Program was reviewed and amended December, 2010.

IDENTIFICATION OF RED FLAGS

A “Red Flag” is a pattern, practice, or specific activity that indicates the possible existence of Identity Theft. In order to identify relevant Red Flags, the City of Columbia considered risk factors such as the types of Records it offers and maintains, the methods it provides to open or establish these Records, the methods it provides to access its Records, and its previous experiences with Identity Theft. The City identified the following Red Flags in each of the listed Categories:

1. Notifications and Warnings from Consumer Reporting Agencies

1) A fraud or activity alert that is included with a consumer report;

2) Receiving a report or notice from a consumer reporting agency of a credit freeze;

3) Receiving a report of fraud with a consumer report; and

4) Receiving indication from a consumer report of activity that is inconsistent with a customer’s usual pattern or activity.

2. Suspicious Documents (see below) used in such a way (items 1-13)

- Lease
- Death certificate
- Driver’s license
- Immigration Papers or Work Card
- Passport
- Birth certificate
- Student Identifications
- Government Issued Identification
- Military Identification
- Non-Driver’s License Identification
- Credit and Debit Cards

1) Receiving documents that are provided for identification that appear to be forged or altered;

2) Receiving documentation on which a person’s photograph or physical description is not consistent with the person presenting the documentation;

3) Receiving other information on the identification not consistent with information provided by the person opening a new Record or customer presenting the identification;

4) Receiving other documentation with information that is not consistent with existing customer information (such as if a person's signature on a check appears forged);

5) Receiving an application for service that appears to have been altered, forged or gives the appearance of having been destroyed and reassembled;

6) Personal identifying information provided is inconsistent when compared against external information sources used by the Department (such as the address does not match any address in the Consumer Report or the Social Security Number has not been issued, or is listed on the Social Security Death's Master File);

7) Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal knowledge and/or external third party sources (telephone number or address on an application is the same as the telephone number or address provided on a fraudulent application;

8) Receiving verbal, written, or internet based information where the same person with the same billing information requests utility service at more than one location;

9) The Social Security Number provided is the same as that submitted by other person(s) opening a Record;

10) The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening Records;

11) The person opening a Record fails to provide all required personal identifying information (incomplete application);

12) The person opening a Record cannot provide authenticating information if requested to do so;

13) The Department is notified by a customer (s) with information that another customer may have opened a fraudulent Record.

3. Suspicious Personal Identifying Information

1) A person's identifying information is inconsistent with other sources of information (such as an address not matching an address on a Consumer Report or a Social Security Number that was never issued);

2) A person's identifying information is inconsistent with other information the customer provides (such as inconsistent Social Security Numbers, billing addresses or birth dates);

3) A person’s identifying information is the same as shown on other applications found to be fraudulent;

4) A person’s identifying information is consistent with fraudulent activity (such as an invalid phone number or a fictitious billing address);

5) A person’s Social Security Number is the same as another customer’s Social Security Number;

6) A person's address or phone number is the same as that of another person;

7) A person fails to provide complete personal identifying information on an application when reminded to do so; and

8) A person’s identifying information is not consistent with the information that is on file for the customer.

9) The physical appearance of a customer does not match with other sources of information (such as driver’s license, passport or immigration work card).

10) A person does not know the last 4 digits of his/her Social Security Number.

11) A new customer requests new service and a routine Social Security Number check locates an account with delinquent or a collection balance that is proved not to be the responsibility of the customer requesting new service.

4. Unusual Use Of or Suspicious Activity Related to a Record

1) A change of address for a Record followed by a request to change the Record holder's name or add other parties;

2) A new Record used in a manner consistent with fraud (such as the customer failing to make the first payment, or making the initial payment and no other payments);

3) A Record being used in a way that is not consistent with prior use (such as late or no payments when the Record has been timely in the past);

4) Mail sent to the Record holder is repeatedly returned as undeliverable;

5) The Department receives notice that a customer is not receiving his paper statements; and

6) The Department receives notice that a Record has unauthorized activity.

7) A Record is designated for shut-off due to non-payment and the customer at the location does not match the customer on file.

8) Unauthorized access to or use of customer records information such as log on or authentication failures**.**

5. Notice Regarding Possible Identity Theft

The City receives notice from a customer, an identity theft victim, law enforcement or any other person that it has opened or is maintaining a fraudulent Account for a person engaged in Identity Theft.

DETECTION OF RED FLAGS.

1. **In order to detect any of the Red Flags identified above with the opening of a new Record, City personnel will take the following steps and verify the identity of the person opening the Record:**

    1) Requiring certain identifying information such as name, date of birth, residential or business address, principal place of business for an entity, Social Security Number, driver's license or other identification;

    2) Verifying the customer's identity in person, such as by copying and reviewing a driver's license or other identification card;

    3) Reviewing documentation showing the existence of a business entity (in person process);

    4) Independently contacting the customer; and

    5) Requesting the customer to appear in person with appropriate information or documentation.

2. **In order to detect any of the Red Flags identified above for an existing Record, City personnel will take the following steps to monitor transactions with such information:**

    1) Verifying the identification of customers if they request information (in person, via telephone, via facsimile, via email);

    2) Verifying the validity of requests to change billing addresses;

    3) Verifying changes in banking information given for billing and payment purposes; and

    4) Verifying the last 4 digits of his/her Social Security Number.

PREVENTING AND MITIGATING IDENTITY THEFT

1. In the event City personnel detect any identified Red Flags, such personnel shall take one or more of the following steps, depending on the degree of risk posed by the Red Flag:

1) Continuing to monitor a Record for evidence of Identity Theft;

2) Person who may be or is suspected to be the possible victim of identity theft;

3) Changing any passwords or other security devices that permit access to Records;

4) Reopening a Record with a new number;

5) Not opening a new Record;

6) Closing an existing Record;

7) Notifying law enforcement; See **Appendix D.**

Example: If the City receives notice that its system has been compromised such that a customer's personal information has become accessible, at a minimum the City will notify the customer and change passwords.

Example: If the City receives notice that a person has provided inaccurate identification information, the Record will be closed immediately and notify Law Enforcement.

8) Determining that no response is warranted under the particular circumstances; or

Example: If the City notices late payments on a Record regularly paid and determines the resident has been incapacitated, no action may be necessary.

9) Notifying the Program Administrator for determination of the appropriate step (s) to take.

2. In order to further prevent the likelihood of identity theft occurring with respect to Records the City will take the following steps with respect to its internal operating procedures:

1) Providing a secure website or clear notice that a website is not secure;

2) Ensuring complete and secure destruction of paper documents and computer files containing customer information. Paper documents and computer files containing customer information should be retained for the minimum retention required by law, unless there is a significant business purpose to retain the record for a longer period of time.

3) Requiring certain provisions included in city contracts with vendors. If the storage or destruction of paper documents and computer files are contracted to a private vendor, contracts must include a provision that requires the private vendor to store the documents and files in a secure manner so as to be accessible only by approved city personnel. Upon appropriate authorization by an approved city official, the vendor shall destroy the documents and computer files in a secure fashion. The storage and destruction of paper documents and computer files which contain sensitive information must be performed by either a city employee or a private vendor under contract.

4) Ensuring that office computers are password protected and that computer screens lock after a set period of time;

5) Requiring only the last 4 digits of Social Security Numbers on customer Records;

6) Requiring each Department review, no less than once a year, employee's access to Record information to determine if the employee's duties require such access and if the employee is complying with the provisions of the City Identity Theft Prevention Program. The Department shall restrict access as much as feasible and maintain an up to date list of those employees required to have access along with the date access was last reviewed. If the employee's access involves computer files, access shall be documented in the City Security Tracking System.

7) Prohibiting Record information to be written on sticky pads or note pads;

8) Ensuring that computer screens are only visible to the employee accessing the Record;

9) Requiring customers to authenticate addresses and personal information, rather than account representatives asking if the information is correct;

10) Maintaining secure office location;

11) Maintaining cameras in timely and good working order and providing for property destruction of tapes and other recording media;

12) Periodically (each Department) reviewing and maintaining a complete, accurate, and current internal list of authorized personnel and procedures with respect to the appropriate responses should a red flag occur or should the Department be aware of actual identity theft. Each Department with

access to such records shall provide periodic reports to the Red Flag Committee and Program Administrator. The report shall include red flags they have detected, their response, and any recommendations for changes in their Department internal policies and procedures and the City Identity Theft Prevention Program.

13) Should vendors have access to personal identifying information, Departments shall also include in contracts with vendors provisions for either the reporting of red flags to the Department or to require the vendor to prevent and mitigate the crime themselves. If the contract provides for the vendor to prevent and mitigate, the contract should also include a provision for periodic reports about the Red Flags the vendor detected and their response.

14) Each city department involved in the opening of new Records or maintenance of existing Records: Utility Customer Services, Parks and Recreation, and Information Systems shall maintain a complete, accurate, and current internal list of authorized personnel with respect to the appropriate responses in the event of a Red Flag occurring, having occurred or an actual Identity Theft; and

14) Because the City cannot predict all particular circumstances that may arise, City Personnel are requested to be diligent while not compromising customer service in the detection of other possible Red Flags.

UPDATING THE PROGRAM AND THE RED FLAGS

1) This Program will be reviewed and updated annually, or as needed, to reflect changes in risks to customers and the soundness of City Records from Identity Theft. An Assistant City Manager will be designated the Program Administrator and work with the **Red Flag Committee,** an internal City working group to consider the City's experiences with Identity Theft, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, changes in types of Records, and changes in the City's business arrangements with other entities. To do so, the Red Flag Committee and Program Administrator shall evaluate the effectiveness of the City Identity Theft Prevention Program, effectiveness of the monitoring of the practices of service providers, and will analyze significant incidents of identity theft and city response.

2) After considering these factors and recommendations from the Committee, the Program Administrator will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Program Administrator will present the Program and recommended changes to the City Council who will make a determination of whether to accept, modify or reject those changes to the Program.

3) Note: Each City Department included in the Program shall conduct an annual Needs Assessment to ensure that their operation is current in identifying Red Flags and response protocol. See Appendix F.

PROGRAM ADMINISTRATION AND TRAINING

1. Oversight.

The City's Program will be overseen by an Assistant City Manager and the Red Flag Committee. Committee members shall consist of the representatives of the City Manager's Office, and all other city Departments that obtain and hold personal identifying information. The Program Administrator will be responsible for the Program's administration, for ensuring appropriate training of staff on the Program, for reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating Identity Theft, determining which steps of prevention and mitigation should be taken in particular circumstances, reviewing and, if necessary, approving changes to the Program.

2. Staff Training and Reports.

City staff responsible for implementing the Program shall be trained under the direction of the Program Administrator, the appropriate Department Head, the Police Department and/or a combination of the above in the detection of Red Flags, and the responsive steps to be taken when a Red Flag is detected. **See Appendix E**. Such training will be sufficient to effectively implement the Program. All training shall be conducted annually and documented. Vendors are required to either report any red flags to the Program Administrator or respond appropriately to prevent and mitigate the crime themselves.

3. Service Provider Arrangements.

The City will take the following steps to ensure the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of Identity Theft.

1) Requiring, by contract, that service providers have such policies and procedures in place;

2) Requiring, by contract, that service providers review the City's Program and report any Red Flags to the Program Administrator; and,

3) Each Department is required to maintain an up-to-date written internal policy as it pertains to their internal security and identity theft.

Patricia Bollmann, Manager
City of Columbia, Utilities and Billing
PO Box 1676
Columbia MO 65205-1676
Phone 573-874-7458
Fax 573-874-7763
E-Mail PAB@gocolumbiamo.com

Appendix A

Finance Department Internal Identity Theft Policy
Utility Customer Services
Effective October 25, 2008

PURPOSE: Establish guidelines consistent with City of Columbia Ordinance

POLICY: Any person or agency requesting information regarding a customer's account must have a demonstrated right to know and present themselves in person with the proper identification.

PROCEDURE:

Customers must identify themselves by the last 4 digits of their SS# before any information may be given on their account. If they can not give the last 4 digits of their SS# no information can be given.

- Telephone requests from the public for phone or social security numbers are always declined
- Persons requesting any information of a personal nature must come in person with picture ID and speak to the Manager/Supervisor.
- Faxed requests for personal information are not acceptable.
- For Realtors or prospective tenants/new homeowners it is acceptable to give information regarding high and low or average utility bills. It is not acceptable to disseminate any personal information in the notes, master file, or payment history.
- Requests for billing information from the file should only be given to the spouse, the significant other, or roommates listed in the master file or notes after they have provided the correct Social Security as verification.
- Governmental agencies; police or prosecutors requesting information should properly identify themselves. These calls should be handled by the Manager or Supervisor or the Collection staff.
- Any discussion of the details of customer's accounts outside of the office is never acceptable for any reason.
- When there is a confidential flag on an account, follow the instructions on the notes

Customer information on master file is password protected.

- Customers are not allowed in CSR Area
- Customer payment agreements are kept in the secure area.
- No paper documents may be left on desks

Janice W. Finley, Business Services Administrator
City of Columbia, Business License Division
PO Box 6015
Columbia MO 65205
Phone: 573-874-7747
Fax: 573-874-7761
E-Mail: Janice@GoColumbiaMo.com

Appendix A (cont'd)

Finance Department Internal Identity Theft Policy
Business License Division
Effective October 25, 2008

PURPOSE: Establish guidelines consistent with City of Columbia Code-4 of Ordinances

POLICY: Any person or agency requesting information regarding a business license customer's confidential information in their license file must have a demonstrated right to know and present themselves in person with the proper identification.

PROCEDURE:

Identification of Red Flags

- Mail sent to the license applicant is repeatedly returned as undeliverable.
- Suspicious immigration papers, criminal background check documents and other identification documents that appear to be forged/altered or are not consistent with information provided by the license applicant.
- Receiving information from American DataBank Inc., the company that provides criminal background check services, concerning the inconsistency of a social security number and date of birth of a license applicant.
- The license applicant fails to provide the required personal identifying information (incomplete application).
- Receiving verbal or written information concerning an applicant submitting fraudulent documents.
- Applicant's driver's license photo is inconsistent with the person presenting the documentation.

- Owner of company listed on license application inconsistent with the Missouri Secretary of State records.

Detection of Red Flags

- Require identifying information from all license applicants.
- Verify the applicant’s identity in person.
- Review documentation showing the existence of a business entity.
- Verify the identity of applicants, if they request information.

Preventing and Mitigating Identity Theft

- American Databank, Inc. monitors identifying information for inconsistencies in social security number, name, date of birth, and relays this information to the Business License Office.
- The invoices received from American Databank include only the last four digits of the applicants’ social security number.
- Applicants’ social security number and business gross receipts information are always deleted/blacked out on documents requested from a licensee’s file.
- Social security and gross receipts information are never released unless requested by the applicant in person upon providing identification.
- Requests for confidential licensing information from City Police Department staff, Law Department staff, representatives from governmental agencies, etc., are required to obtain this information from the Business Services Administrator after providing identification.
- Inactive business license files are stored in a locked area.
- All Business License staff computers are password protected.
- Computer screens are only visible to the Business License employee when accessing licensing records.
- File cabinets that contain business license records, as well as hotel/motel and cigarette tax records, are locked at the end of each business day. The Business License area is never left unattended during office hours and access to this area is restricted to Business License staff and management.

- Always obtain copy of applicant’s driver’s license or other picture ID when applying for a license or permit.

- Check immigration papers to ensure validity.

- If an applicant fails to provide the requested personal identifying information, the license or permit application is denied.

- The appearance of altered or forged documents prompts further investigation.

- Double check with Missouri Secretary of State’s Office to confirm members of a corporation are consistent with those listed on the application.

- Obtain criminal background check from previous state in which the applicant resided if the applicant has lived in Missouri for less than one year.

- Computer screen darkens or fades out when staff is away from their desks.

- The Business Services Administrator is the only person who can grant access to the business license system.

Ron Barrett, Comptroller
City of Columbia, Accounting Division
PO Box 6015
Columbia MO 65205
Phone: 573-874-7371
Fax: 573-874-7686
E-Mail: Ron@GoColumbiaMo.com

Appendix A (cont'd)

Finance Department Internal Identity Theft Policy
Miscellaneous Receivables Accounting Division
Effective October 25, 2008

PURPOSE: Establish guidelines consistent with City of Columbia Code of Ordinances

POLICY: Any person or agency requesting information regarding a miscellaneous receivables customer's confidential information in their miscellaneous receivables file must have a demonstrated right to know

PROCEDURE:

Identification of Red Flags

- Mail sent to the miscellaneous receivable customer is repeatedly returned as undeliverable.

- Suspicious immigration papers, criminal background check documents and other identification documents that appear to be forged/altered or are not consistent with information provided by the miscellaneous receivable customer.

- Receiving verbal or written information concerning a miscellaneous receivable customer submitting fraudulent documents.

- Owner of company listed on miscellaneous receivable customer inconsistent with the MO Secretary of State records.

Detection of Red Flags

- Review documentation showing the existence of a business entity.

- Verify the identity of miscellaneous receivable customer if they request information.

Preventing and Mitigating Identity Theft

- Social security numbers are never requested, used, or stored, in the miscellaneous receivable customer information system

- Requests for confidential miscellaneous receivable customer information files are provided only to city staff that are working with the miscellaneous receivable customer information as required for their department

- Customers' bank account information which is stored in the miscellaneous receivable system is maintained in a secure manner. This information is not disclosed to parties outside the miscellaneous receivable system staff.

- Inactive miscellaneous receivable customer files are stored in a locked area.

- All miscellaneous receivable customer system records are password protected.

- The appearance of altered or forged documents prompts further investigation.

- Computer screen darkens or fades out when miscellaneous receivable staff is away from their desk.

- The Accounting Assistant for miscellaneous receivables is designated as the only person who can grant access to the miscellaneous receivable system

APPENDIX B

Parks and Recreation Records Internal Identity Theft Policy
Effective October 20, 2008

PURPOSE: Establish guidelines consistent with the City of Columbia's Identity Theft Prevention Program.

POLICY: Any person or agency requesting information regarding customer's personal information must have a demonstrated right to know and present themselves in person with the proper identification.

PROCEDURE:

- All credit card and ACH banking information stored in RecTrac database is encrypted throughout the database and cannot be obtained by any user or staff.
- WebTrac (online registration) user name and passwords are set by customer. If customer forgets this information, they must know their security features they set up in order to access such information.
- E-mail and phone requests requesting customer's PIN # for online registration must confirm their mailing address, phone number and security features.
- Faxed requests are not acceptable.
- Refunds and payments are only allowed by the actual customer. There shall be no refunds or transfers of programs by individuals outside the customer's household.
- Governmental agencies; police or prosecutors requesting information must properly identify themselves. These requests should be handled by the Manager or Supervisor.
- Any discussion of the details of customer's personal information outside of the office is never acceptable for any reason.
- Scholarship assistance information shall be stored in a lockable file cabinet. Access to scholarship information shall be limited to those employees requiring access.
- The Department shall maintain an up-to-date list of those employees that are required to have access to personal records.
- Any photocopies made by Manager or Supervisor must have sensitive information (social security number, driver license number) blacked out.

APPENDIX C

Information Systems Internal Identity Theft Policy
Effective April 3, 2008

Relevant excerpts from the
City of Columbia Comprehensive Security Policy
(entire policy may be found online at
http://www.columbia.mo.gov/is/documents/security-policies.pdf)

1.3 Identification and Authentication

1.3.1 Passwords

Passwords confirm that a person is who they claim to be. As such, passwords are extremely important to the security of the City of Columbia Information System. In general, city password policy encourages a balance between complexity, rotation, and user needs. Both lenient and strict policies are generally counter productive to security. This policy instead strives to set standards that, when used together, strike an appropriate balance.

1.3.1.1 Complexity

Passwords should be greater than 8 characters, mix upper and lower case characters, and use symbols. Alternatively, passphrases can be used in the absence of passwords. For example, “AskNotForWhomTheBellTolls” is a very long password and is therefore more difficult to break. Passwords should not be easily guessed. Phone numbers, names of friends, relatives, and pets, and other personal information are generally very easy to guess.

PCI DSS 8.5.10

1.3.1.2 Rotation

Passwords should not resemble previous passwords. For example, “Password12” should not be used if “Password11” has been used before. Where possible, systems and applications should be set to “remember” old passwords and disallow use of passwords that match or are similar to a previous password. Where possible, systems should be set to store the last 10 passwords.

PCI DSS 8.5.12

1.3.1.3 Password Responsibilities of Users

Users are responsible for choosing passwords that are reasonably complex as defined in 1.3.1.1. Users must be able to use their passwords day to day and are therefore responsible for choosing passwords that will be meaningful enough for them to remember. Users are allowed to write down their password if they are unable to remember it. If a user chooses to write down his/her password, he/she must follow these rules:

a) Their user id must not accompany the password

b) The written password must be stored in a locked location to which ONLY the user has access. The written password must never be hidden in an unlocked location.

c) The password should not be disposed of until it is no longer valid. If possible, the user should shred the password.

Users must recognize the importance of password privacy. Users must never share their password with anyone. Users must never ask each other for their passwords. Departments must make sure that business operations are such that users never need to share credentials. IT staff must never ask users for their passwords and users must understand that IT staff will never do so.

1.3.1.4 Creating and resetting passwords

Temporary passwords, whether created due to account creation or password reset, are subject to section 1.3.1.1. A temporary password created for one user should not be the same as a temporary password created for another user. Instead, temporary passwords should be random and unique.

Users should call the Helpdesk to have passwords reset for every system and application. The Helpdesk should generate a temporary password, set the password to expired, and give the user the new password. The Helpdesk should encourage the user to immediately change the password. When passwords are reset the password should never be available to the user in an electronic form. The Helpdesk shall reset the password then give the new password to the user over the phone.

When a user requests a password reset, a work order shall be immediately created before continuing. The technician resetting the passwords shall check the SecTrack application to ensure the user is allowed to use the system for which he/she is requesting the password change. If the user is not authorized to use the system for which he/she is requesting access, the technician shall inform the user that he/she needs access through the SecTrack system and he/she should speak to his/her supervisor. The success or failure of the password reset will be documented in the work order. The temporary password should not be put in the content of the work order.

Users should never be allowed to reset their password without sufficiently proving that they are who they claim to be. Systems and applications that have “Forgot Password” links should direct users to the Helpdesk instead of providing a password reset method. Helpdesk employees must take responsibility for ensuring that the person requesting a password change is who they claim to be.

If the helpdesk employee cannot verify the user's identity, the Helpdesk employee may require the user to provide "cognitive passwords," or answers to questions that only the user is likely to know. A list of questions and their corresponding answers will be maintained by the IT department, and when a user calls with a password reset request, three questions will be chosen at random. The user must be able to answer the cognitive password questions before the password is reset.

PCI DSS 8.5.2, PCI DSS 8.5.3

1.3.1.5 Password expire

Passwords shall expire every 90 days. Once a password is expired, the user shall be required to change it. All systems and applications that support password expiration should enforce this policy.

PCI DSS 8.5.9

1.3.1.6 Password Transmission and Storage

Passwords should be encrypted using hash algorithms whenever stored or transmitted. The password hash algorithm used should be evaluated in accordance with the cryptography policy.

PCI DSS 8.4

1.4.3 User privilege audits

Each system and application should have a user privilege audit at least annually. The audit should consist of two parts:

1) Department confirmation that the requested access on file in SecTrack matches the access the department wishes the user to have.

2) The access given matches the access requested in SecTrack.

Satisfies NERC CIP-003-1 R5.2

1.4.4 Account audits

Each system and application should have an account audit at least annually. The audit may be done in concert with the user privilege audit in 1.4.3. The audit should consist of two parts:

1) Enumeration of all user accounts.

2) Determination that each user account has a valid SecTrack request and that the user is still employed by the city.

NERC CIP-003-1 R5.2

1.5 Accountability and risk mitigation measures

1.5.1 Accountability

Every system and application has an accountability mechanism that differs in some way from the mechanisms of other systems and applications. Each system and applications should be evaluated and accountability mechanisms should be enabled and configured according to risk. The following are general guidelines to implementing accountability across multiple independent systems and applications.

1.5.2 Authentication logging

Systems and applications should, where possible, create log entries for authentication attempts, both successful and failed. Log entries should include user identification, date/time stamp, and the device (machine name and/or IP address) from which the attempt originated.

1.5.3 Review of authentication events

Every system and application should have its logs reviewed regularly for possible security breaches. The frequency and content of the log audits may be different for each system and should be risk based.

1.5.4 Last login information

On systems and applications where capability exists, the user should be presented with details about their last successful login. Details should include time, date, place and any other pertinent information specific to the system or application.

1.6 Administration

1.6.1 Clipping level

Accounts should not allow an infinite number of “tries” until the correct password is used. Instead systems and applications should implement a “clipping level” that locks out accounts once a certain number of failed attempts has occurred for a user id. Systems and applications that have an enforcement mechanism for this policy shall have this value set to no more than 6. If possible, the user should not be aware that their account is disabled, only that their login attempt failed. Systems and applications should lock accounts for no less than 30 minutes.

PCI DSS 8.5.13, PCI DSS 8.5.14

APPENDIX D

Columbia Police Department Notification Procedures
Effective October 24, 2008

City of Columbia Employees will routinely be exposed to situations where Identity theft is a concern. It is imperative that staff follow notification procedures to ensure that the interests of both the City of Columbia and potential victims are protected.

Employees will consistently be discussing account and customer information over the phone or in person. It is imperative that the customer identity be established prior to any account services being provided. Employees, at times, will be given conflicting or false customer information. If the information can not be clarified or substantiated by staff to a reasonable degree, the customer will be required to respond in person and show a valid form of photo I.D. Once employees are reasonably satisfied there are no identity theft concerns, services can be provided.

Employees who continue to suspect the customer of identity theft can request the assistance of the Columbia Police Department. Employees should obtain a detailed description of the suspect and be able to provide a short synopsis of the incident. Officers will respond to investigate, determine if a crime occurred and take appropriate action.

Staff will potentially discover instances of identity theft or will be notified by a customer of the crime. Employees will assist victims of identity theft with necessary information and also assist with the investigation. Employees will provide an “Identity Theft Victim Information” sheet to all potential victims. Any victims who suffer a monetary loss and are seeking potential reimbursement from the city of Columbia will be required to file a police report and assist with prosecution.

Employees will call the Columbia Police Department and an officer will respond to investigate. Staff should be prepared to provide the officer copies of original documents or any other pertinent information that can be used for the investigation. If the City of Columbia suffers a loss from the identity theft incident the officer needs to note this in the police report for potential restitution.

Employees discovering incidents of internal theft should obtain enough information for a preliminary police report. Staff should be prepared to work with investigators and gather the following information:

Case preparation guideline for embezzlement or internal theft cases

Major Crimes Division, Columbia Police Department

No one is more familiar with your bookkeeping methods than you or your accountant. Therefore, it is important that you convey that information in a manner that is easy to understand and follow. In order to assist in the investigation and prosecution of your case, it is requested that you provide documentation in the following format.

Document preparation:

When preparing your documentation, place all of the pertinent information into a three-ringed binder that is designed to hold your information secure. Original documents should be used when compiling your initial folder. Once your original binder has been completed, make three copies. Please retain one copy for your records. The original and **two** copies should be submitted to the police. Once your case has been completed, the original documents will be returned to you. **Please remember that a neat and professional product is very important.**

Overview sheet:

The overview is a “brief” narrative that provides enough details of the case that the reader can obtain a clear understanding of the incident. The following information must be included, but is not limited to:

A. Who discovered the theft and how it was uncovered.
B. Who the suspect is.
C. The dates of when the theft started and ended.
D. The theft amount.
E. How the theft was performed.
F. The names of anyone the suspect made statements to about the theft and what was said.

Narrative sheet:

Please provide a “detailed” explanation of the theft. Please include the same information from the Overview Sheet section, plus an explanation of the supporting evidence, i.e. documents, ledgers, receipts, etc. Note: This section should read like a novel, covering every aspect of the case from beginning to end. Your information may be returned for revision, if this section is not thorough. It is vital that you explain all the supporting documents in this section, so it is clear and easy to understand. All documents must be numbered. Numbering each document makes it easier for the reader to locate information, when you refer to specific figures and page numbers. You may also consider using a highlighter to aid in quick location of figures.

Itemized list

This section is composed of an itemized list of each loss, date of the loss and the supporting document page number. A total loss dollar amount should be included at the bottom of this list.

Supporting Documents:

Include all documents relating to this case, which were explained in the “Narrative” section. **If you have any questions; do not hesitate to call the detective handling your case. The investigative office can be reached at (573) 874-7423.**

Finally, employees discovering incidents of computer related crimes (hacking or similar offenses) or where customer information or employee identity theft is at risk should immediately call the Columbia Police Department to file a report and initiate an investigation. (**Emergency 911**; **Non-Emergency 442-6131)**

The following Identity Theft Victim Information is what responding police officers provide Identity Theft Victims:

Identity Theft Victim Information

The City of Columbia requires a Police report and cooperation in the prosecution of the person or persons responsible before any reimbursement of losses will be discussed/determined.

Place a fraud alert on your credit reports and review your credit reports:

Equifax 1-800-525-6285
P.O. Box 740241
Atlanta, GA 30374-0241

Experian 1-888-EXPERIAN (397-3742)
P.O. Box 9532
Allen, TX 75013

TransUnion 1-800-680-7289
Fraud Victim Assistance Division
P.O. Box 6790
Fullerton, CA 92834-6790

When you report to one of these bureaus, they will report to the other two for you, and send you free reports. When you receive your reports, review them carefully. If there are any errors, report that to the credit bureaus by phone and in writing.

Close any accounts that have been tampered with or opened fraudulently, such as credit cards, bank accounts, phone and cell phone accounts, utility accounts, and internet service providers. Either use an Identity Theft Affidavit or ask the company to
send you fraud dispute forms if they prefer, if there are fraudulent charges or debits.

The ID Theft Affidavit is to make sure you do not become responsible for debts incurred by the ID thief, so you must provide proof you did not create the debt. You can use the affidavit where a NEW account was opened in your name. Use it ASAP. For EXISTING accounts, your credit company will provide you with their own Dispute forms. The ID Theft Affidavit can be found at www.consumer.gov/idtheft.

If your ATM card is lost, stolen, or otherwise compromised, cancel it. Get a new card and PIN.

If your checks were stolen or misused, close that account and open a new one. Contact the three major check verification companies, and ask that retailers who use their databases not accept your checks.

TeleCheck 1-800-710-9898 or 927-0188

Certegy, Inc.	1-800-437-5120
International Check Services	1-800-631-9656

Call SCAN at 1-800-262-7771 to see if bad checks are being passed in your name.

- **File a complaint with the FTC.**

FTC Toll-free 1-877-IDTHEFT (438-4338), www.consumer.gov/idtheft TDD 202-326-2502

Identity Theft Clearinghouse
Federal Trade Commission
600 Pennsylvania Ave., NW
Washington, DC 20580

- Document everything: Keep originals of all correspondence and documents; send copies as necessary

- Keep a record of everyone you talk to (names, dates, etc.)

- Keep all your files FOREVER! If something happens at a later date, you will be glad you did

- If you believe someone has filed for bankruptcy in your name, write to the U.S. Trustee in the region where it was filed. A list is available on the UST website at www.usdoj.gov/ust/

- If wrongful criminal violations are attributed to your name, contact that law enforcement agency

- Contact the Department of Motor Vehicles at www.dor.mo.gov/ and ask that your files be flagged

- If theft of mail was involved, contact the U.S. Postal Inspection Service at www.usps.gov/websites/depart/inspect

- If phone fraud was involved, contact the Public Utility Commission. If cell phone or long distance service was involved, contact the FCC at www.fcc.gov

- If your social security number was involved, contact the Social Security Administration at www.socialsecurity.gov

- If tax fraud was involved, contact the IRS at www.treas.gov/irs/ci

- **You can find much more information about Identity Theft, with more help and guidance, at the FTC's website at www.consumer.gov/idtheft**

- ***Information provided comes directly from the FTC's website at www.consumer.gov/idtheft***

Appendix E

Identity Theft Training Program
Effective December 1, 2008

Training Protocol

I. Introduction

a. What is Identity Theft?

II. Red Flag Legislation

a. The Federal Trade Commission's Red Flag Rule (Implements Section 114 of the Fair and Accurate Credit Transaction Act of 2003, pursuant to 16 C.F.R. 681.2.
b. Complying with the Red Flag Rule
c. How flexible is the Red Flag Rule?

III. The City's Identity Theft Prevention Program

a. Departments who must comply
b. Examples of Red Flags
c. What is your role and responsibility?

IV. Identity Theft

a. What is Identity Theft?
b. How does it happen?
c. How do you protect yourself from it?
d. What do you do if you're a victim?

V. How to Report

a. Your expectations
b. Notifying Law Enforcement
c. Your Assistance if investigation involved
d. What to do if a Law Enforcement response is not necessary

VI. Resources

Appendix F

Needs Assessment
Effective December 1, 2008

Conducting a Needs Assessment

Opening a New Record

Identify the steps in establishing a new record for a customer.

1) What identification is required? How do you obtain identifying information and verify identity? ______________________________
____
____
____

2) Do they need to make the application in person or can they send in the information in an alternate form? Telephone or other? ______________________________
____
____
____

3) Does the Department use consumer reports in the application process? How? Establish deposit? Approve or deny services? ______________________________
____
____
____

4) Does the Department have policies and procedures that define red flags for identity theft and actions for mitigation? ______________________________
____
____
____

5) What happens to the hand written notes made by the Department Representative in the application process? ______________________________
____
____
____

6) Is the computer screen visible to others during the application process? ____________
____
____
____

7) Who has access to data once entered? Does the Department Representative lock computer when not at desk? ______________________________
____
____
____

8) If applicant gives address, bank account, date of birth or social security number verbally to Department Representative, what precautions are taken from others hearing? ____

____

____

9) Once personal identification information is entered by Department Representative, where and how can it later be retrieved? ________________________________

____

10) What safeguards are currently built into the application process? ______________

____

____

____

11) What safeguards would you like to implement? __________________________

____

____

____

12) Which employees have access to information – is it on a “need to know” basis? _____

____

____

____

13) Is any customer personal information carried into the field on a laptop? _________

____

____

____

Map out the steps that occur when opening a new account. Is customer identification validated? Is so, how? Trace the flow of secured information.

Customer Initial Contact

Service is established

Needs Assessment continued

Monitoring an Existing Record

Identify the possible red flags that may exist in the following procedures:

- ✓ Authenticating transactions for existing customers
- ✓ Monitoring activity/transaction of customers
- ✓ Verifying the validity of change of billing address
- ✓ Does the Department have policies and procedures that define red flags for identity theft and action for mitigation for existing records?

Does your Department use passwords or some form of security access?

____
____
____
____

Describe your process for verifying validating the following:

Check by phone____

Credit Card Number____

Are receipts ever printed? If so, what part of number is exposed?__________________

In what manner have customers attempted to fraudulently represent themselves as someone else in a transaction in an existing account?

____

What safeguards are currently built into monitoring existing record(s)?

____
____
____
____

What safeguards would you like to implement?

____
____
____
____

Map out the ways customers, 3rd parties and others access existing Records.

How do you authenticate transactions for existing Records?

Request

Request Fulfilled

After you have mapped out the flow of information, identify possible areas where the protection of secured information could be improved.