



CITY COUNCIL ACTION REPORT

TO: John Szerlag, Acting City Manager

FROM: John M. Lamerato, Assistant City Manager/Finance & Administration
James A. Nash, Financial Services Director
Gert Paraskevin, Information Technology Director
Sandra Kasperek, City Treasurer
Stephen Cooperrider, Risk Manager

SUBJECT: Agenda Item – Adoption of the City of Troy Identity Theft Prevention Program in Compliance with the Fair and Accurate Credit Transaction (FACT) Act of 2003 as amended November 9, 2007.

Background:

- The Federal Trade Commission (FTC) issued an amendment to the FACT Act in 2007 to provide new protections to consumers against the growing problem of identity theft.
- The FTC requires that creditors with covered accounts must implement a written Identity Theft Prevention Program.
- The FTC has determined that utilities are covered accounts and that municipalities are considered creditors in this regard.
- The FACT Act amendment requires the creation of a Privacy Committee (Risk Manager, IT Director, City Treasurer, Water Department - Office Coordinator, Police Department representative) to draft the policy and implement it.
- The FACT Act requires the written Identity Theft Prevention Program to be adopted by the governing board by May 1, 2009.
- The City of Troy has always acted to protect the personal identification information of our citizens. The attached Program document developed by the Privacy Committee serves to formalize practices already in place.

Financial Considerations:

- Failure to implement a written policy can result in civil penalties of up to \$2,500 per violation.

Legal Considerations:

- The City must be in compliance with the FACT Act rules as promulgated.

Policy Considerations:

- Troy enhances the health and safety of the community.
- Troy is rebuilding for a healthy economy reflecting the values of a unique community in a changing and interconnected world.

Options:

- The Privacy Committee and City Management recommend the adoption of the Identity Theft Prevention Program as submitted.

City of Troy - Public Utility

Identity Theft Prevention Program

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 and to provide for continued administration of the Program in compliance with the Federal Trade Commission's Red Flags Rule (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.

Under the Red Flag Rule, every financial institution and creditor is required to establish an "Identity Theft Prevention Program" tailored to its size, complexity and the nature of its operation. Each program must contain reasonable policies and procedures to:

- Identify relevant Red Flags and incorporate them into the Program;
- Detect Red Flags;
- Respond appropriately to any Red Flags that are detected to prevent and mitigate Identity Theft; and
- Ensure the Program is updated periodically, to reflect changes in risks to customers or to the safety and soundness of the creditor from Identity Theft.

DEFINITIONS

Personal Identification Information means any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including:

- Name
- Address
- Telephone number
- Social Security Number (SSN)
- Date of Birth (DOB)
- Government issued Driver's License, ID or Passport
- Employer or Taxpayer Identification Number
- Internet Protocol address, or routing code
- Credit Card Number
- Personal Identification Number (PIN)
- Bank Account Number
- Utility Account Number

Identify theft is fraud committed using identifying information of another person without authority.

A **red flag** means a pattern, practice or specific activity that indicates the possible existence of identity theft.

SCOPE

1. This policy applies to all City of Troy employees as it relates to utility accounts, and contractors of the City of Troy.
2. This policy supplements but does not replace existing policies.

POLICY

PROCEDURES FOR OPENING A NEW ACCOUNT

In Person/by mail:

1. Obtain sufficient Personal Identification Information to allow you to form a reasonable belief that the customer is who they claim to be, including, but not limited to:
 - a. Name
 - b. Service Address
 - c. Phone Number
 - d. Name of Financial Institution
 - e. Checking/Savings Account Number
 - f. Routing Number
2. Avoid taking Personal Identification Information verbally when other customers can overhear the conversation. Information provided must be in writing.
3. Ensure that City Employee computer monitors are not visible to others.
4. Check for Red Flags. (See Appendix A: Examples of Red Flags). If a Red Flag is detected, follow the prescribed Next Step in the Red Flag check list. If you are unsure of the Next Step, consult with your supervisor before processing the request for the new account. Red Flags must be resolved before a new account can be established.

By Telephone:

1. City employee does not provide information by telephone. Customer must provide information in writing.
2. Check for Red Flags (See Appendix A: Examples of Red Flags). If a Red Flag is detected follow the prescribed Next Step in the Red Flag check list. If you are unsure of the Next Step, consult with your supervisor before processing the request for a new account. Red Flags must be resolved before a new account can be established.

PROCEDURES FOR EXISTING ACCOUNTS

1. Watch for Red Flags whenever executing transactions on customer accounts.
2. Caller must provide the account information. Employee does not provide any account information to caller.

3. A change of mailing address initiated by the customer requires the same level of authentication as opening a new account. Customers must provide personal identification to establish a billing address different than the customer account address.
4. Safeguard all credit card information, checks, ACH information, bankruptcy statements or other personal financial information at all times. These documents should be stored in a secure location until they can be properly destroyed consistent with the Records Retention and Disposal Schedule.

GENERAL SECURITY GUIDELINES

1. All employees with access to customer utility account personal identification information are required to complete the Identity Theft Prevention Program training and complete an annual update.
2. Ensure complete and secure destruction of paper documents and computer files containing customer information.
3. Ensure that passwords are difficult to determine.
4. Ensure that office computer screens lock and are password protected.
5. Follow proper computer shutdown or screen locking procedures before leaving work stations.
6. Ensure that customers Personal Identification Information is not left on computer screens longer than necessary to execute transactions.
7. Ensure that desks and workstations are clear of papers containing customers Personal Identification Information.
8. Ensure computer virus protection is up to date.
9. Require and keep only the kinds of customer information that are necessary for utility purposes.

RESPONSE TO BREACH OF SECURITY

In the event personnel detect any identified Red Flags, personnel should not confront any individual suspected of committing identity theft. It is only their duty to report any suspected patterns of identity theft. Depending on the degree of risk posed by the Red Flag, personnel shall take one or more of the following steps:

1. Continue to monitor an account for evidence of Identity Theft.
2. Contact the customer.
3. Change any passwords or other security devices that permit access to accounts.
4. Not open a new account or close an existing account.
5. Notify the City Treasurer for determination of the appropriate step(s) to take.
6. The City Treasurer may notify law enforcement if situation warrants.

ADMINISTRATIVE PROCEDURES

The Risk Manager (Privacy Officer), with assistance from the Privacy Committee shall:

1. Develop and implement reasonable policies and procedures for an Identity Theft Prevention Program that complies with federal guidelines implementing the FACT Act.
2. Insure all supervisors and employees involved in utility accounts receive the necessary training to effectively implement the Program.
3. Establish a contact at the Troy Police Department to report suspected cases of identity theft.
4. Receive reports of Red Flags that require mitigation.
5. Conduct periodic risk assessments of the Program.
6. Periodically review and update the Program procedures and Appendix A – Examples of Red Flags.
7. Insure continued compliance with the FACT Act.
8. Call meetings of the Privacy Committee as needed to review Policy and Procedures.

Stephen Cooperrider, Risk Manager / Privacy Officer Dated _____

James A. Nash, Financial Services Director

John M. Lamerato, Assistant City Manager/Fin. & Admin.

Approved by _____
John Szerlag, Acting City Manager

Dated

APPENDIX A – EXAMPLES OF RED FLAGS

I. SUSPICIOUS DOCUMENTS

- Identification document or card that appears to be forged, altered or not authentic.
- Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document.
- Other document with information that is not consistent with existing customer information (example: person's signature on a check appears forged).
- Application for service that appears to have been altered or forged.

Next Step:

1. In all cases, advise the customer that there appears to be a discrepancy with their documentation and they will need to provide verification of their identity before the transaction can be completed.
2. In some cases, it may be necessary to contact the landlord or property owner to verify who the tenant is.

Mitigation:

1. In all cases, do not open a new account until you are satisfied that the customer is who they claim to be. If necessary, request further documentation (check stub or W-2). Where appropriate attempt to contact the person named on the documents and advise them that they may be the victim of an attempted identity theft. If the matter is not reasonably resolved, advise a supervisor. In some instances, management may need to close an existing account and/or contact the Troy Police Department.

II. SUSPICIOUS PERSONAL IDENTIFICATION INFORMATION

- Identifying information presented that is inconsistent with other information the customer provides (example: different name).
- Identifying information presented that is inconsistent with other sources of information (example: an account number not matching an account number on record).
- Identifying information presented that is the same as information shown on other applications that were found to be fraudulent.
- Identifying information presented that is consistent with fraudulent activity (example: invalid phone number or fictitious billing address).

Next Step:

1. Advise the customer there appears to be a discrepancy with their documentation and they will have to provide validation of their identity before the transaction can be completed.

2. In the case of an address discrepancy, require the customer to bring in proper documentation such as a picture ID, pay stub or W2. You must be satisfied the address is correct before proceeding with the transaction.

Mitigation:

1. Contact the customer, do not open a new account or close an existing account until you have validated the customer's identity.

- An address or phone number presented that is the same as that of another person.

Next Step:

1. Ask customer to verify address / phone number and / or bring in Photo ID.

Mitigation:

1. Do not proceed with any transaction if there is doubt about a customer's identity.

- A person fails to provide complete personal identifying information on an application or in response to notification that an application is incomplete.

Next Step:

1. Check the billing system for any other customers that may have made a similar attempt to obtain service at that address and ask customer to bring in photo ID.

Mitigation:

1. Do not proceed with any transaction if there is doubt about a customer's identity.

III. SUSPICIOUS ACCOUNT ACTIVITY OR UNUSUAL USE OF ACCOUNT

- Change of address for an account followed by a request to change the account holder's name.
- Payments stop on an otherwise consistently up-to-date account.
- Account used in a way that is not consistent with prior use (example: very high activity).
- Mail sent to the account holder is repeatedly returned as undeliverable.
- Notice that a customer is not receiving mail sent by the City of Troy.
- Notice that an account has unauthorized activity.

Next Step:

1. Review the account, check for notes and check to see if the customer has been in contact with us.

Mitigation:

1. Contact the customer and advise them of the unusual activity.

IV. NOTICE FROM CUSTOMERS, VICTIMS OF IDENTITY THEFT, LAW ENFORCEMENT AUTHORITIES OR ANY PERSONS REGARDING POSSIBLE IDENTITY THEFT

- The City of Troy is notified by a customer, victim of identity theft, law enforcement authority or any other person that the City of Troy has opened a fraudulent account for a person engaged in identity theft.

Next Step:

1. Get a copy of the police report and check with the customer to validate their ID and check for accuracy and errors.
2. Review to determine if the account should be closed.

Mitigation:

1. Possibly close the account. Contact the customer; change any passwords, security codes or other devices that permit access to the account. Do not attempt to collect on an account, and do not sell it.

SPECIFIC PROGRAM ELEMENTS AND CONFIDENTIALITY

For the effectiveness of Identity Theft Prevention Programs, the Red Flag Rule envisions a degree of confidentiality regarding the City of Troy's specific practices relating to Identity Theft detection, prevention and mitigation. Therefore, under this Program, knowledge of such specific practices shall be limited to the Privacy Committee and those employees who need to know them for purposes of preventing identity theft. Because this Program is to be adopted by a public body and thus publicly available, it would be counterproductive to list these specific practices here. Therefore, only the Program's general red flag detection, implementation and prevention practices are listed in this document.