AGENDA ITEM SUMMARY
FORT COLLINS CITY COUNCIL

ITEM NUMBER: 23

DATE: April 21, 2009

STAFF: Fran Seaworth

SUBJECT

Resolution 2009-036 Approving and Adopting an Identity Theft Prevention Program of the City's Municipal Court for the Detection, Prevention and Mitigation of Identity Theft.

RECOMMENDATION

Staff recommends adoption of the Resolution.

FINANCIAL IMPACT

The financial impact of implementation will be minimal to Municipal Court operations.

EXECUTIVE SUMMARY

Under the revisions to the FACT Act of 2003 (Fair and Accurate Credit Transactions Act), each creditor is required to have policies and procedures in place by May 1, 2009 which meet the standards outlined by Federal Agencies including the Federal Trade Commission. There are a number of red flags or potential warnings of identity theft included in current legislation. The role of the Council acting as the City's Board of Directors is to grant initial approval of the Identity Theft Program plan before implementation and annual report review. The program includes the following:

- Establish a Privacy Officer
- Conduct a Needs Assessment
- Develop an Annual Program Report
- Develop and Implement Policies and Procedures
- Employee Training – 2 Hours in First Year

BACKGROUND

The FACT Act (2003) was passed to set standards for guarding customer information. On November 1, 2007, the red flags rules (the "Red Flags Rules") were adopted by the Federal Trade Commission to hold creditors accountable for the prevention, detection and mitigation of identity theft. The Municipal Court is included in the red flag legislation because the Court extends credit to defendants with misdemeanor violations who are unable to pay fines at the time judgment is entered and would like to enter into agreements to pay their fines over time. This constitutes the maintenance of ongoing accounts primarily for personal purposes and the accounts are designed to

accept multiple payments. The Municipal Court is responsible for developing an identity theft prevention program designed to prevent identity theft and to protect the personal information of those who sign up for this form of credit.

Municipal court staff has begun the process of establishing and implementing written policies and procedures, conducting needs assessments, and training employees. A Privacy Officer has been designated and assigned the responsibilities of coordinating the policies and procedures established to comply with the Red Flags Rules. The Privacy Officer responsibilities are described in the attachment.

ATTACHMENTS

1. Privacy Officer.

FORT COLLINS MUNICIPAL COURT IDENTITY THEFT PROGRAM
PRIVACY OFFICER
APRIL, 2009

I. Privacy Officer

The Municipal Court Supervisor will serve as the Privacy Officer for the Municipal Court and, due to the small size of the court staff, will assume all responsibilities necessary for meeting the requirements of the Red Flags Rules.

II. Responsibilities of Privacy Officer

1. Complete components of needs assessment
2. Design and develop assigned policies and procedures
3. Program evaluation
4. Updates
5. Employee training
6. Periodic "walk-through" to assess compliance and look for strategies to enhance prevention, identification and mitigation of red flags.
7. Preparation of reports of program effectiveness:
    - Focus on outcomes
    - Highlight the steps/precautions used
    - City Council – annual report review

RESOLUTION 2009-036
OF THE COUNCIL OF THE CITY OF FORT COLLINS
APPROVING AND ADOPTING AN IDENTITY THEFT PREVENTION PROGRAM
OF THE CITY'S MUNICIPAL COURT FOR THE DETECTION, PREVENTION AND
MITIGATION OF IDENTITY THEFT

WHEREAS, the Fair and Accurate Credit Transactions Act of 2003 (the "Act") requires several federal agencies including the Federal Trade Commission to establish guidelines for use by creditors regarding identity theft prevention; and

WHEREAS, on November 9, 2007, the Federal Trade Commission published final rules, set forth in 16 CFR Part 681, (the "Red Flags Rules") requiring that creditors create and implement a program to address the detection, prevention and mitigation of identity theft; and

WHEREAS, the City's Municipal Court (the "Court") is a "creditor" and carries "covered accounts" as those terms are defined in the Red Flags Rules when the Court extends credit to defendants with misdemeanor violations who are unable to pay their fines at the time that judgment is entered; and

WHEREAS, Court staff has prepared a program to address the detection, prevention and mitigation of identity theft for the Court's covered accounts, which program is attached hereto as Exhibit "A" (the "Identity Theft Program"), and the Court intends to implement such program in compliance with the Red Flags Rules; and

WHEREAS, the Red Flags Rules require Court staff to obtain City Council approval of the initial Identity Theft Program; and

WHEREAS, in Court staff's opinion, the Identity Theft Program meets the requirements of the Red Flags Rules and equips the Court with the necessary guidance to continue its efforts to detect, prevent and mitigate identity theft related to covered accounts and will hereafter be available to the public in the office of the City Clerk.

NOW, THEREFORE, BE IT RESOLVED BY THE CITY COUNCIL OF THE CITY OF FORT COLLINS that upon review and consideration of the Identity Theft Program, the City Council hereby finds that such program is in the best interests of the City of Fort Collins and hereby approves and adopts said program.

Passed and adopted at a regular meeting of the Council of the City of Fort Collins this 21st day of April A.D. 2009.

_____
Mayor

ATTEST:

_____
City Clerk

EXHIBIT "A"

City of Fort Collins Municipal Court
Identity Theft Prevention Program
April, 2009

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 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.

Definitions

Identity theft means fraud committed or attempted using the identifying information of another person without authority.

A **covered account** means:

1. An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions. Covered accounts include credit card accounts, mortgage loans, automobile loans, margin accounts, cell phone accounts, utility accounts, checking accounts and savings accounts; and

2. Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation or litigation risks.

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

The Program

The City of Fort Collins Municipal Court 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; and

4. Ensure the Program is updated periodically to reflect changes to risks to customers and to the safety and soundness of the creditor from identity theft.

The program shall, as appropriate, incorporate existing policies and procedures that control reasonably foreseeable risks.

Administration of the Program

1. The Municipal Court Supervisor 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.

Identification of Relevant 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, 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 or 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 about, and verifying the identity of, a person opening a covered account; and

2. Authenticating customers, monitoring transactions, and verifying the validity of change of address requests in the case of existing covered accounts.

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. Contact the customer;
3. Change any passwords, security codes or other security devices that permit access to a covered account;
4. Reopen a covered account with a new account number;
5. Not open a new covered account;
6. Close an existing covered account;
7. Notify law enforcement; or
8. Determine no response is warranted under the particular circumstances.

Updating the Program

The Program shall be updated periodically to reflect changes in risks to customers or to the safety and soundness of the court from identity theft based on factors such as:

1. The experiences of the court with identity theft;
2. Changes in methods of identity theft;
3. Changes in methods to detect, prevent and mitigate identity theft;
4. Changes in the types of accounts that the court offers and maintains.

Oversight of the Program

1. Oversight of the Program shall include:

    a. Assignment of specific responsibility for implementation of the Program;
    b. Review of reports prepared by staff regarding compliance; and
    c. Approval of material changes to the Program as necessary to address changing risks of identity theft.

2. Reports shall be prepared as follows:

    a. Staff responsible for development, implementation and administration of the Program shall report to the City Council at least annually on compliance by the court with the Program.

    b. The report shall address material matters related to the Program and evaluate issues such as:
        i. The effectiveness of the 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;
        ii. Service provider agreements;
        iii. Significant incidents involving identity theft and management's response; and
        iv. Recommendations for material changes to the Program.

Oversight of Service Provider Arrangements

The court 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 court engages a service provider to perform an activity in connection with one or more covered accounts.