

RESOLUTION NO. 11-34

**A RESOLUTION OF THE CITY COUNCIL OF THE CITY OF CASTLE PINES,  
COLORADO ADOPTING A POLICY PERTAINING TO  
IDENTITY THEFT PREVENTION**

WHEREAS, the Federal Trade Commission has adopted new federal rules, known as the "Red Flag Rules," that mandate the creation of identity theft prevention programs for all affected financial institutions and creditors; and

WHEREAS, under the Red Flag Rules, financial institutions and creditors must develop a written program that identifies and detects the relevant warning signs or "red flags" of identity theft; and

WHEREAS, the Federal Trade Commission has confirmed that the Red Flag requirements apply to all municipal utilities and other municipal operations which provide services or products before billing the customer thus making them a creditor as defined under the Red Flag Rules; and

WHEREAS, the City of Castle Pines may be deemed a creditor under the Red Flag Rules as it offers certain municipal services for which payments are some times received after the service has been provided; and

WHEREAS, the City Council desires to adopt a written policy on the detection, prevention and mitigation of identity theft in conformance with the Red Flag Rules.

NOW, THEREFORE, BE IT RESOLVED BY THE CITY COUNCIL OF THE CITY OF CASTLE PINES, COLORADO, THAT:

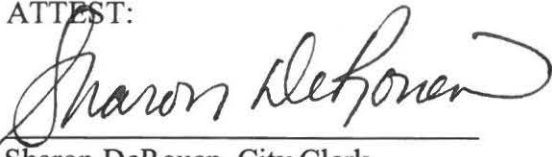
Section 1. The City Council hereby approves and adopts the attached Policy titled "Red Flag Policy and Identity Theft Prevention Program."

Section 2. **Effective Date.** This Resolution is effective upon adoption.

INTRODUCED, READ AND ADOPTED AT A REGULAR MEETING OF THE CITY COUNCIL OF THE CITY OF CASTLE PINES by a vote of 7 in favor and 0 against this 24<sup>th</sup> day of May, 2011.

  
\_\_\_\_\_  
Jeffrey T. Huff, Mayor

ATTEST:



Sharon DeRouen, City Clerk

APPROVED AS TO FORM:



Linda C. Michow, City Attorney

# CITY OF CASTLE PINES, COLORADO

## Red Flag Policy and Identity Theft Prevention Program

### I. Purpose

The purpose of this Policy and Program is to evaluate the foreseeable risk of Identity Theft associated with Covered Accounts maintained by the City of Castle Pines and to establish an appropriate Identity Theft Prevention Program designed to detect, prevent and mitigate Identity Theft in connection with the opening or maintenance of any Covered Account. Through this Policy and Program, the City Council will also administer the Program in compliance with Part 681 of Title 16 of the Code of Federal Regulations (CFR) implementing Sections 114 and 315 of the Fair and Accurate Credit Transactions (FACT) Act of 2003.

### II. Definitions

1. *City* means the City of Castle Pines, Colorado.
2. *City Manager* means the City Manager appointed by the City Council or his or her designee.
3. *Covered Account*, for purposes of this Policy, shall mean (i) accounts opened and/or maintained for building permit and inspections, land use applications, municipal court, and open records photocopying and research; and (ii) any other account that the City offers or maintains for which there is a reasonably foreseeable risk to Customers or to the safety and soundness of the City from Identity Theft.
4. *Credit* means the right granted by the City to a Customer for payment of debt or to incur debts and defer its payment or to purchase City services or property and defer payment therefore.
5. *Creditor* means any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit and includes utility companies and telecommunications companies.
6. *Customer* means a person that has a Covered Account with the City.
7. *Identity Theft* means a fraud committed or attempted using identifying information of another person without authority.
8. *Personal Identifying Information* means a person's credit card account information, debit card information, bank account information and drivers' license information and for a natural person includes their social security number, mother's birth name, and date of birth.

9. *Red Flag* means a pattern, practice, or specific activity that indicates the possible existence of Identity Theft.

### **III. Findings**

1. The federal rules mandating the creation of Identity Theft prevention programs known as the “Red Flag Rules” under the Fair and Accurate Credit Transactions (“FACT”) Act of 2003 apply to financial institutions and Creditors as those terms are defined under the FACT Act.
2. The definition of Creditor under the FACT Act, and as interpreted by the Federal Trade Commission, includes all municipal utilities and other municipal operations which provide services or products in advance of billing the Customer.
3. The City Council finds that the City may be deemed a Creditor under the FACT Act due to its provision of municipal services for which payment is or may be made on Credit.
4. The municipal services provided by the City for which payment is or may be made on Credit include: photocopying, retrieval and research services by the City Clerk’s Office under the Colorado Open Records Act; building plan reviews, inspections and re-inspections; development services provided to Customers through the Community Development Department; municipal court; and any other municipal services for which the City accepts payment on Credit.
5. The City Council finds there is no reasonably foreseeable risk of Identity Theft in connection with its Covered Accounts as no Personal Identifying Information of its Customers is collected or maintained by the City in opening and maintaining its Covered Accounts. Further, the City has had no reports of Identity Theft with respect to any of its Covered Accounts.
6. Based on the foregoing findings, the City Council determines that the Identity Theft Prevention Program herein provided is appropriate to the nature of its Covered Accounts and the scope of the City’s management of the same.

### **IV. Program Administration**

The City Manager is responsible for oversight, development, implementation and administration of the Program, including the provision of training as deemed necessary by the City Manager to all employees responsible for or involved in opening or accepting payment for a Covered Account with respect to the implementation and requirements of the Identity Theft Prevention Program.

### **V. Management of Covered Accounts**

- A. Access. Access to Covered Account information shall be limited to authorized City personnel.
- B. Payments.
  1. In the event that any payments are made through a third party service provider, such third party service provider shall certify to the City that it has an adequate Identity Theft prevention program in place that is applicable to such payments.

2. Account statements and receipts for Covered Accounts shall include only the last four digits of the credit or debit card or the bank account used for payment of the Covered Account.

C. Sources and Types of Red Flags.

All employees responsible for or involved in the process of opening a Covered Account or accepting payment for a Covered Account shall check for Red Flags as indicators of possible Identity Theft, such as:

1. Suspicious documents, including but not limited to: documents provided for identification that appear to be altered or forged; identification on which the photograph or physical description is inconsistent with the appearance of the applicant or Customer; identification on which the information is inconsistent with information provided by the applicant or Customer; identification on which the information is inconsistent with readily accessible information that is on file with the City, such as the application for service; or an application that appears to have been altered or forged.
2. Unusual use of or suspicious activity relating to a Covered Account.
3. Receipt of a notice from Customers, law enforcement, victims or other reliable sources regarding possible Identity Theft relating to Covered Accounts.

**VI. Prevention and Mitigation of Identity Theft**

The City and its employees, contractors, and agents shall exercise all reasonable means and care to maintain the security of its Covered Accounts and shall respond appropriately to the detection of Red Flags. The City Manager shall periodically assess the risks of Identity Theft.

**VII. Updating the Program**

The City Manager shall periodically review and, as deemed necessary, update the Identity Theft Prevention Program in conformance with the federal Red Flag guidelines issued by the Federal Trade Commission.