CITY OF CHESAPEAKE, VIRGINIA **NUMBER: 1.27**

ADMINISTRATIVE REGULATION **EFFECTIVE DATE: 05/24/10**

SUBJECT: CITY MANAGER'S OFFICE
IDENTITY THEFT PROTECTION PROGRAM

I. Purpose:

The following program is adopted in order to establish policy regarding the design, implementation and administration of written identity theft prevention procedures within the affected departments of the City of Chesapeake. These identity theft prevention procedures shall provide for the identification, detection, and response to patterns, practices, or specific activities – (known as "Red Flags")– that could indicate identity theft. The City of Chesapeake intends to comply fully with the Fair and Accurate Credit Transactions Act of 2003 (FACTA).

II. ASSIGNMENT OF RESPONSIBILITIES

A. City Manager

The overall responsibility and authority for the Identity Theft Protection Program lies with the City Manager or his designee. The City Manager's office or his designee shall oversee the Program and make policy changes as he/she deems necessary. The City Manager or his designee shall also appoint a Program Administrator to implement the Program and assure compliance with this regulation.

B. Department Heads

1. Each affected department head shall be responsible for the development, administration, and monitoring of written Identity Theft Prevention Procedures within his/her department and maintaining records for examination by the City Auditor. The Program shall be tailored to the size, complexity and nature of the specific department based upon a documented risk assessment of identity theft in the department.

2. Each affected department head shall provide the leadership, supervision and follow up which is essential in maintaining firm identity theft prevention procedures.

3. Staff from the affected departments responsible for implementing the Procedures shall be trained in the detection of Red Flags and the responsive steps to be taken when a Red Flag is detected.

4. Each affected department head shall assure compliance with the Fair and Accurate Credit Transactions Act of 2003 as well as the related Federal, State, and local laws, orders, and policies.

5. Each affected department head shall annually prepare a report for the City Manager's Office or his designee, in which he/she updates the risk assessment of identity theft and evaluates the effectiveness of the procedures, significant incidents involving identity theft and responses, and recommendations for changes to the procedures.

6. Each unaffected department which handles monetary transactions shall annually have it's department head provide a statement for the City Manager's Office, or his designee, certifying that, to the best of their knowledge, no identity theft problems have been noted or reported.

III. PROCEDURE REQUIREMENTS

A. Identify relevant Red Flags for new and existing Covered Accounts and incorporate those Red Flags into the Procedures;

B. Detect Red Flags that have been incorporated into the Procedures;

C. Respond appropriately to any Red Flags that are detected to prevent and mitigate Identity Theft; and

D. Ensure the procedures are updated periodically, to reflect changes in risks to customers/citizens or to the safety and soundness of the creditor from Identity Theft.

IV. METHODOLOGY TO ACCOMPLISH PROCEDURE REQUIREMENTS

In order to identify relevant Red Flags, the affected departments consider the types of accounts that it offers and maintains, the methods it provides to open its accounts, the methods it provides to access its accounts and its previous experience with Identity Theft.

Accounts impacted by FACTA ("Covered Account") are:

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

The affected departments identify Red Flags from various sources such as:

A. Notifications and Warnings from Credit Reporting Agencies
B. Suspicious Documents (forgery, inconsistencies, etc.)
C. Suspicious Personal Identifying Information
D. Suspicious Account Activity or Unusual Use of Account
E. Alerts From Others

The affected departments shall have adopted steps to detect Red Flags in both new and existing accounts.

The affected departments shall have adopted steps to prevent and mitigate Identity Theft and protect identifying information received from citizens and customers.

William E. Harrell, City Manager

5/24/10
Date