

RED FLAG RULES

I. PURPOSE:

The following guideline establishes policies and procedures to detect warning signs of identity theft in day-to-day operations, steps to prevent the crime and mitigate the damage it inflicts.

II. DEFINITION:

This guideline shall apply to all City Departments who receive payments for services.

Background: The Federal Trade Commission (FTC) requires every creditor to implement an Identity Theft Prevention Program (ITPP). The FTC requirement and regulation is necessary because of Section 114 of the Fair and Accurate Credit Transactions Act. The FTC has set forth the ITPP requirement in 16 C.F.R. Subsection 681.2.

III. PROCEDURES:

- A. The first step is to identify red flags. Red flags may consist of suspicious documents:
 - 1. Presentation of documents appearing to be altered or forged.
 - 2. Presentation of photographs or physical descriptions that are not consistent with the appearance of the applicant or customer.
 - 3. Presentation of other documentation that is not consistent with the information provided when the account was opened or existing customer information.
 - 4. Presentation of information that is not consistent with the account application.
 - 5. Presentation of an application that appears to have been altered, forged, destroyed or reassembled.

- B. Red flags may also consist of suspicious personal identifying information:
 - 1. Personal identifying information is being provided by the customer that is not consistent with other personal identifying information provided by the customer or is not consistent with the customer's account application.

2. Personal identifying information is associated with known fraudulent activity.
3. The social security number, if required or obtained, is the same as that submitted by another customer.
4. The telephone number or address is the same as that submitted by another customer,
5. The applicant failed to provide all personal identifying information requested on the application.
6. The applicant or customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

C. Red flags may also consist of unusual use of or suspicious activity related to an account:

1. A change of address for an account followed by a request to change the account holder's name.
2. A change of address for an account followed by a request to add new or additional authorized users or representatives.
3. An account is not being utilized in a way that is consistent with prior utilization, such as late or no payments when the account has been timely in the past.
4. A new account is utilized in a manner commonly associated with known patterns of fraudulent activity, such as customer fails to make the first payment or makes the first payment but no subsequent payments.
5. Mail sent to the account holder is repeatedly returned as undeliverable.
6. Certified Mail sent to eh account holds and not signed.
7. The City receives notice that a customer is not receiving his paper statements.
8. The City receives notice of unauthorized activity on the account.

D. Red flags may also consist of notice regarding possible identity theft:

1. Notice from a customer, an identity theft victim, law enforcement personnel or other reliable sources regarding possible identity theft.

E. Any customer opening an account must provide proof of identity along with a signed application. Said proof may include, but not be limited to: a valid driver's license; passport; State or Federal identification card; or military identification card.

F. All personal information, personal identifying information, account applications and account information collected and maintained by the City shall be a confidential record of the City and shall not be subject to disclosure unless otherwise required by State or Federal Law.

G. Access to account information shall be limited to employees that provide customer service to the City. Any computer that has access to customer


information shall be password protected and shall be locked when the employee steps away from the workstation. All paper and non-electronic based customer information shall be stored and maintained in a locked room or cabinet and access should be limited.

- H. Credit card transactions shall only be processed by a third party processor that complies with all appropriate credit card processing requirements of the card issuer or the Payment Card Industry (PCI). Credit card payments made to the City shall comply with the merchant agreement and/or card holders' agreement.
- I. Suspicious transactions include, but are not limited to, the presentation of incomplete applications; unsigned applications; payment by someone other than the individual named on the account; presentation of inconsistent signatures, addresses or identification.
- J. Department Directors of the City shall ensure that any suspicious transactions that occurs within their Department will be reported to the Compliance Officer. The Compliance Officer shall utilize his/her discretion on whether to report suspicious transactions to the Little Rock Police Department, or other appropriate law enforcement agency.

IV. ACCOUNTABILITY:

- A. An annual report, as required by FTC regulations, shall be provided by the Compliance Officer to the Board of Directors. The contents of the annual report shall address and/or evaluation at least the following:
 - 1. The effectiveness of the policies and procedures of the City in addressing the risk of identity theft in connection with the opening of accounts and with respect to access to existing accounts.
 - 2. Credit-card processing and service provider arrangements.
 - 3. Incidents involving identity theft or suspected identity theft and the City's response.
 - 4. Any changes or proposed changes in methods of identity theft and the prevention of identity theft.
 - 5. Recommendations for changes to the City's ITPP.

Approved:



Bruce T. Moore
City Manager