CITY OF WEST ALLIS

POLICY AREA 1 - GENERAL

CP 2008-1.11 Identity Theft Prevention & Red Flag Alerts

Adopted **April 21, 2009**

1.11.010 Purpose of Policy

Pursuant to the Fair and Accurate Credit Transaction Act (FACTA) provisions of the federal Fair Credit Reporting Act , the City of West Allis (City) must take appropriate measures to safeguard Personal Identifying Information and Covered Accounts from Identity Theft. The purpose of this policy shall be to identify the City's response when patterns, practices, or specific activities occur that indicate the possible existence of Identity Theft and to take all reasonable steps to prevent, and mitigate the theft of Personal Identifying Information. As general guidance, this policy will apply to any City account, program, or procedure which allows multiple household or personal payments or collects, transfers, stores, or records a person's personally identifiable information.

1.11.020 Definitions

1.11.021 Covered Accounts are accounts the City offers or maintains for personal, family, or household purposes that involve multiple payments or transactions and include deferred payments for services or property. Covered Accounts may include utility accounts, ambulance accounts, lien/loan accounts or any customer account where the extension of credit is offered resulting in a continuing relationship and therefore subject to provisions of the Fair and Accurate Credit Transaction Act of 2003.

1.11.022 Identity Theft is a fraud committed or attempted using the Personal Identifying Information of another person without authority.

1.11.023 Personal Identifying Information is any person's first name and last name in combination with any other information, that can be used to identify a specific person, so long as the information obtained would be sufficient to permit a person to commit Identity Theft against the person whose information was compromised. Other information may include but not be limited to a Social Security Number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number or address.

1.11.024 Red Flag is a pattern, practice or specific activity that indicates the possible existence of Identity Theft.

1.11.030 Policy

Pursuant to State and federal law, the City shall adopt the following general administrative rules to identify and detect Red Flags that raise concerns that Personal Identifying Information or Covered Account information is potentially being misused or stolen and outline procedures for safeguarding this information. The policy shall include eight primary areas of compliance:

- Personal Identifying Information
- Covered Accounts
- Red Flags
- Safeguarding Personal Identifying Information
- Third Party Vendors
- Notice of Theft
- Notice of Security Breach
- Policy Implementation

1.11.040 Personal Identifying Information

The City collects a substantial amount of Personal Identifying Information through multiple processes requiring staff to assess and address risks associated with the collection of this information. Departments are responsible for assessing current compliance and documenting appropriate safeguard practices in writing.

1.11.050 Covered Accounts

Covered Accounts may include utility accounts or any customer account where the extension of credit is offered resulting in a continuing relationship. Covered Accounts or any other account where there may be a reasonably foreseeable risk to customers from Identity Theft are subject to provisions of the Fair and Accurate Credit Transaction Act which requires the City to take additional precautions to eliminate the threat of Identity Theft. Before a customer can open an account with the City, staff must make a good faith attempt to verify the identity of the person opening the account. Prospective applicants who wish to receive a specific service must provide Personal Identifying Information as required by staff.

1.11.060 Red Flags

Red Flag patterns, practices or specific activities that indicate the possible existence of Identity Theft may include alerts, notifications, or other warnings received from local law enforcement or other governmental organizations. Such information may include a fraud alert or the United States Post Office providing a

notice of address discrepancy. Categories of Red Flags associated with customer accounts or the ability to initiate a customer account may include:

- inquiries inconsistent with the history and usual pattern of activity of a customer including such things as a recent and significant increase in the volume of inquiries;
- an unusual number of recently established credit relationships;
- a material change in the use of services, or other unusual activity associated with the account;
- an account that was closed for cause or identified for abuse of account privileges;
- documents provided for identification that appear to have been altered or forged;
- the photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification;
- other information on the identification is not consistent with information provided by the person opening a new account or customer presenting the identification;
- other information on the identification is not consistent with readily accessible information that is on file, such as a prior customer file; or
- an application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Other potential Red Flags such as the presentation of suspicious information that may include Personal Identifying Information that is inconsistent when compared against other information sources such as:

- an address that does not match any address in the financial system data file;
- a Social Security Number that does not match previous history for the same customer;
- Personal Identifying Information provided by the customer that is not consistent with other Personal Identifying Information provided by the customer;
- Personal Identifying Information provided is associated with known fraudulent activity as indicated by internal or third-party sources;
- an address on an application is the same as the address provided on a fraudulent application;
- a phone number on an application is the same as the number provided on a fraudulent application;
- Personal Identifying Information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources;
- an address on an application is fictitious, a mail drop, or a prison;

- a phone number that is invalid, or is associated with a pager or answering service;
- a Social Security Number provided is the same as that submitted by other persons opening an account or other customer;
- an address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers;
- a person opening the account fails to provide all required Personal Identifying Information on an application or in response to notification that the application is incomplete;
- Personal Identifying Information provided is not consistent with information that is on file with the City; or
- the person opening the account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report in response to a challenge question.

Unusual or suspicious activity may include:

- shortly following the notice of a change of address for a customer account, the City receives a request for the addition of authorized users on the account;
- mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's Covered Account;
- the City is notified that the customer is not receiving their bill;
- payments are made in a manner associated with fraud; or
- an existing account with a stable history shows irregularities.

The policy shall provide appropriate responses to detected Red Flags to prevent and mitigate Identity Theft. The City Administrative Officer, IT Manager, the Department Manager, and the City Attorneys office will determine an appropriate response commensurate with the degree of risk posed.

1.11.070 Safeguarding Personal Identifying Information

The City shall implement and maintain reasonable safeguards to protect the security and confidentiality of Personal Identifying Information, including its proper disposal. In the event a report indicates an information discrepancy, the discrepancy will be reported to the supervisor for further review and verification of the information, including verifying identification in person at the City, if necessary.

Staff shall also report to their supervisor when it appears that account documents have been altered or forged when compared to other documents in a customer or

employee file. It shall be brought to a supervisor's attention immediately if any customer, employee or applicant presents invalid identification, or identification that appears forged for the purpose of obtaining access to account information.

Access to account information will be permitted in person at the City, only after verifying the person's identity through photo identification or by providing information known only to that person. Account information can also be obtained over the Internet with secure password protection. Access to customer account information via telephone or Internet shall require the customer to verify his or her identity using information that would only be known to the customer as reflected in the customer's account. Staff will notify their supervisor and make note in a customer's file when there is a lack of correlation between information provided by a customer and information contained in a file for the purposes of gaining access to account information. Information will not be given without first clearing any discrepancies in the information provided.

In addition, staff will no longer request Personal Identifying Information on certain forms if the data is determined no longer needed for operational purposes. Documents that have reached retention periods will be purged and destroyed in a manner that maintains Personal Identifying Information in a secure manner. Documents with Personal Identifying Information will be stored in locking files or behind locked doors. Any documents containing Personal Identifying Information will be destroyed or shredded prior to disposal.

Staff will note unusual use of accounts, or suspicious activities related to accounts and promptly notify their supervisor when there are an unusually high number of inquiries on an account, coupled with a lack of correlation in the information provided by the customer or employee.

When a supervisor is notified of a discrepancy, the supervisor will immediately contact (by telephone or email) the City Administrative Officer, IT Manager, the Department Manager, and the City Attorneys office. The supervisor will then submit a Red Flag Discrepancy Report detailing the event, to the City Administrative Officer, IT Manager, the Department Manager, and the City Attorneys office within 24 hours. The City Administrative Officer, IT Manager, the Department Manager, and the City Attorneys office will determine an appropriate response commensurate with the degree of risk posed. The supervisory form for reporting potential red flag discrepancies is attached hereto and made a part of the Policy hereof.

Printing Social Security Numbers on any mailed materials unless redacted; or on cards used to access products, services, or City buildings (such as ID cards); or publicly posting or displaying Social Security Numbers is prohibited. Exemptions include requirements by the state of Wisconsin; federal laws, including statute,

such as W2s, W4s, 1099s, etc; records that are required by law to be made available to the public; records for use for internal verification or administrative processes; and records used for enforcing a judgment or court order.

Staff will monitor transactions and verify the validity of change of address requests, in the case of existing accounts. Social Security Numbers or Tax Identification Numbers will not be provided by staff either verbally or in writing, even where a customer is asking for his/her own information.

If the City discovers that any of its customers or employees have become a victim of Identity Theft through Personal Identifying Information used by the City in opening or maintaining an account or associated with any document, the City Administrative Officer, IT Manager, the Department Manager, and the City Attorneys office will take appropriate steps that it deems necessary to mitigate the impacts of such Identity Theft.

The City Administrative Officer, IT Manager, and the City Attorneys office group [IS Manager in consultation with the City Administrative Officer and City Attorney's Office] is responsible to safeguard Personal Identifying Information stored in electronic format and to document safeguard practices in writing.

1.11.080 Third Party Vendors

The City has various business relationships with third party contractors. Under these business relationships, the third party contractor may have access to customer information covered under this policy. The City will ensure that the third party contractor's work for the organization is consistent with this policy by:

- amending City contracts to incorporate these requirements; or
- by determining through written acknowledgment that the third party contractor has reasonable alternative safeguards that provide the same or a greater level of protection for Personal Identifying Information as provided by the organization.

1.11.090 Notice of Theft

Notice from customers or employees, victims of Identity Theft, law enforcement authorities, or other persons regarding possible Identity Theft in connection with customer or employee information can potentially be a Red Flag for Identity Theft. Upon notice of Identity Theft to a supervisor, the City Administrative Officer, IT Manager, the Department Manager, and the City Attorneys office will be notified to determine an appropriate response commensurate with the degree of risk posed.

1.11.100 Notification of Security Breach

In the event that Personal Identifying Information has been subject to a security breach, City Administrative Officer, IT Manager, or the City Attorneys office will notify the Police Department.

1.11.110 Implementation

The Human Resources Division is responsible to include this Identity Theft Protection and Red Flag Alert Policy as part of new employee orientation by documenting review of this policy and the concepts.

Department Managers are responsible to be familiar with the Identity Theft Protection Acts and to meet with their staff to assess current compliance and document appropriate safeguard practices in writing.

Employees are responsible to comply with this policy and any internal processes as directed by their department. Noncompliance may result in formal disciplinary action up to and including termination of employment. Employees should contact their supervisor if they have questions about compliance with this policy.

The Finance Division is responsible to audit departments on an annual basis for compliance verification. A security checklist will be provided to each department to act as a guideline to ensure compliance and proper procedures are followed. The checklist will include sections on program elements, employees, safeguarding electronic information, vendor compliance, and information storage and disposal. Upon review and compliance with the checklist, each department must return a signed copy to the Finance Department.

The City Administrative Officer, IT Manager, Human Resources Manager, Finance Manager and the City Attorneys office are responsible for oversight of the program and program implementation.

1.11.120 Review and Update

As new ways are discovered to perpetrate Identity Theft, organizations subject to the Red Flag Rules must establish reasonable policies and procedures to ensure that the organizations' Identity Theft Prevention Policy is updated periodically to reflect changes in risks to customers, employees and to the safety of the organization.

This policy shall be reviewed annually in October by the City Administrative Officer, IT Manager, and the City Attorneys office and updated as necessary.