THE CITY OF LAKE FOREST **Administrative Directive 3-4**
Office of the City Manager **May 2025**

Identity Theft Policy

I. POLICY PURPOSE

This Policy is to help protect employees, customers, contractors, and the City from harm and damage related to, or caused by, the loss or misuse of sensitive information. The Policy also will assist the City in detecting, preventing, and mitigating identity theft. The Policy does so by identifying certain "red flags" that suggest or indicate the possibility of identity theft, and by providing guidelines on how the City should respond once it detects any such Red Flags. Further, the Policy will:

1. Define sensitive information;
2. Describe the physical security of data when it is printed on paper;
3. Describe the electronic security of data when stored and distributed; and
4. Place the City in compliance with state and federal law regarding identity theft protection.

The policy also covers the Identity Protection Act (5ILCS179), which took effect June 1, 2010.

The Policy has been tailored to the size, complexity and the nature of the City's operations. The Policy also has been designed in order to:

1. Identify relevant Red Flags for new and existing covered accounts and incorporate those Red Flags into the Policy;

2. Detect Red Flags that have been incorporated into the Policy;

3. Allow the City to respond appropriately to any Red Flags that are detected to prevent and mitigate Identity Theft; and

4. Ensure that the Policy is reviewed periodically, and updated, if necessary, to reflect changes in risks to customers or to the safety and soundness of the City from identity theft.

Policies specific to Payment Card Industry (PCI) compliance are supplemental to this policy and are contained in a separate Administrative Directive.

II. POLICY DEFINITIONS

1. "Covered Account" means: (i) an account that the City offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a utility account; 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, including financial, operational, compliance, reputation, or litigation risks.

2. "Credit" means the right granted by a creditor to a debtor to defer payment of debt or to incur debts and defer its payment or to purchase property or services and defer payment therefore.

3 "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, including utility companies.

4. "Customer" means a person that has a covered account with a creditor.

5. "Identity Theft" means a fraud committed or attempted using identifying information of another person without authority.

6. "Person" means a natural person, a corporation, government or governmental subdivision or agency, trust, estate, partnership, cooperative, or association.

7. "Sensitive Information" means any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including, but not limited to, a person's credit card account information, debit card information, bank account information, drivers' license information, social security number, mother's birth name, date of birth, electronic identification number, computer Internet Protocol address, and routing code.

8. "Red Flag" means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

9. "Service Provider" means a person that provides a service directly to the City.

III. IDENTIFICATION OF RED FLAGS.

In order to identify relevant Red Flags, the City considers 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 experiences with Identity Theft. The City identifies the following Red Flags, in the following listed categories:

A. Notifications and Warnings from Credit Reporting Agencies

Red Flags

1. Report of fraud accompanying a credit report;

2. Notice or report from a credit agency of a credit freeze on a customer or applicant;

3. Notice or report from a credit agency of an active duty alert for an applicant; and

4. Indication from a credit report of activity that is inconsistent with a customer's usual pattern or activity.

B. Suspicious Documents

Red Flags

1. Identification document or card that appears to be forged, altered or otherwise inauthentic;

2. Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;

3. Other documentation with information that is not consistent with existing customer information (*e.g.* a person's signature on a check appears forged); and

4. Application for service that appears to have been altered or forged.

C. Suspicious Personal Identifying Information

Red Flags

1. Identifying information presented that is inconsistent with other information the customer provides (*e.g.* inconsistent birth dates);

2. Identifying information presented that is inconsistent with other sources of information (*e.g.* an address not matching an address on a credit report);

3. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;

4. Identifying information presented that is consistent with fraudulent activity (*e.g.* an invalid phone number or an answering service, or fictitious billing address, mail drop or prison);

5. Social security number presented that is the same as one given by another customer;

6. An address or phone number presented that is the same as that of another person;

7. A person fails to provide complete personal identifying information on an application when reminded to do so; and

8. A person's identifying information is not consistent with the information that is on file for the customer.

D. Suspicious Account Activity or Unusual Use of Account

Red Flags

1. Change of address for an account followed by a request to change the account holder's name;

2. Payments stop on an otherwise consistently up-to-date account;

3. Account used in a way that is not consistent with prior use (*e.g.* very high activity);

4. Mail sent to the account holder is repeatedly returned as undeliverable;

5. Notice to the City that a customer is not receiving mail sent by the City;

6. Notice to the City that an account has unauthorized activity;

7. Breach in the City's computer system security; and

8. Unauthorized access to or use of customer account information.

E. Alerts from Others

Red Flag

1. Notice to the City from a customer, identity theft victim, law enforcement or other person that it has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.

IV. DETECTING RED FLAGS.

A. New Covered Accounts

In order to try and detect any of the Red Flags identified above associated with the opening of a new Covered Account, City personnel should take the following steps to obtain and verify the identity of the person opening the Covered Account:

1. Require certain identifying information such as name, date of birth, residential or business address, principal place of business for an entity, driver's license or other identification;

2. Verify the customer's identity (*e.g.* review a driver's license or other identification card);

3, Review documentation showing the existence of a business entity; and

4. Independently contact the customer if appropriate.

B. Existing Covered Accounts

In order to detect any of the Red Flags identified in Section V above for an existing Covered Account, City personnel will take the following steps to monitor transactions with a Covered Account:

1. Verify the identification of customers if they request information (in person, via telephone, via facsimile, via email, or otherwise);

2. Verify the validity of requests to change billing addresses; and

3. Verify changes in banking information given for billing and payment purposes.

V. PREVENTING AND MITIGATING IDENTITY THEFT

A. Securing Sensitive Information

City personnel are encouraged to use common sense judgment in securing sensitive and confidential information. Furthermore, in exercising such judgment, consideration should be given to the Illinois Freedom of Information Act ("FOIA"). If an employee is uncertain of the sensitivity of a particular piece of information, the employee should contact their supervisor or the Policy Administrator. Further, if the City receives a FOIA or other request seeking Sensitive Information, or documents containing Sensitive Information, said requests should be forwarded to the City Manager and the City Attorney.

In order to further prevent the likelihood of Identity Theft occurring with respect to City accounts, the City shall make reasonable efforts to take the following steps with respect to its internal operating procedures to protect customer identifying information:

1. Take steps to ensure that the City's website is secure or provide clear notice that the website is not secure;

2. Attempt to ensure destruction of paper documents and computer files containing Sensitive Information;

3. Keep file cabinets, desk drawers, cabinets, and any other storage space containing documents with Sensitive Information locked when not in use;

4. Lock storage rooms containing documents with Sensitive Information and record retention area when not in use.

5. Attempt to ensure that office computers with access to Covered Accounts and/or Sensitive Information are password protected and that computer screens lock after a set period of time;

6. Keep workstations, work areas, and offices clear of papers containing Sensitive Information;

7. Request only the last 4 digits of social security numbers (if any);

8. Attempt to ensure that computer virus protection is up to date;

9. Require and keep only the kinds of Sensitive Information that are necessary for the City's purposes; and

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

B. Electronic Distribution

Each employee, service provider, or contractor performing work for the City will comply with the following policies:

1. With respect to internal electronic distribution, Sensitive Information may be transmitted using approved City electronic mail.

2. With respect to external electronic distribution, Sensitive Information should only be transmitted in an encrypted format and should contain a statement such as this:

   "This message may contain sensitive, confidential and/or proprietary information and is intended for the person/entity to whom it was originally addressed. Any use by others is strictly prohibited".

3. With respect to electronic distribution of Sensitive Information, credit/debit card information may never be electronically distributed once received by the City, either internally or externally.

C. Responses When Red Flags Detected

In the event City personnel detect any identified Red Flags, such personnel should take one or more of the following steps, depending on the degree of risk posed by the Red Flag:

1. Continue to monitor an account for evidence of Identity Theft;
2. Contact the customer;
3. Change any passwords or other security devices that permit access to Covered Accounts;
4. Decline or otherwise refuse to open a new Covered Account;
5. Close an existing Covered Account;
6. Reopen a Covered Account with a new number;
7. Notify the Policy Administrator for determination of the appropriate step(s) to take;
8. Notify law enforcement; or

9. Determine that no response is warranted under the particular circumstances.

VI. ILLINOIS IDENTITY PROTECTION ACT

A. In compliance with the Identity Protection Act, the City prohibits any employee from doing the following:

1. Publicly post or publicly display in any manner an individual's social security number.
2. Print an individual's social security number on any card required for the individual to access products or services provided by the City.
3. Require an individual to transmit his or her social security number over the Internet, unless the connection is secure or the social security number is encrypted.
4. Print an individual's social security number on any materials that are mailed to the individual, through the U.S. Postal Service, any private mail service, electronic mail, or any similar method of delivery, unless State or federal law requires the social security number to be on the document to be mailed. Notwithstanding any provision in this Section to the contrary, social security numbers may be included in applications and forms sent by mail, including, but not limited to, any material mailed in connection with the administration of the Unemployment Insurance Act, any material mailed in connection with any tax administered by the Department of Revenue, and documents sent as part of an application or enrollment process or to establish, amend, or terminate an account, contract, or policy or to confirm the accuracy of the social security number. A social security number that may permissibly be mailed under this Section may not be printed, in whole or in part, on a postcard or other mailer that does not require an envelope or be visible on an envelope without the envelope having been opened.
5. Collect, use, or disclose a social security number from an individual, unless (i) required to do so under State or federal law, rules, or regulations, or the collection, use, or disclosure of the social security number is otherwise necessary for the performance of that agency's duties and responsibilities; (ii) the need and purpose for the social security number is documented before collection of the social security number; and (iii) the social security number collected is relevant to the documented need and purpose.
6. Require an individual to use his or her social security number to access an Internet website.
7. Use the social security number for any purpose other than the purpose for which it was collected.

The prohibitions set forth in items 5-7 do not apply in the following circumstances:

1. The disclosure of social security numbers to agents, employees, contractors, or subcontractors of a governmental entity or disclosure by a governmental entity to another governmental entity or its agents, employees, contractors, or subcontractors if disclosure is necessary in order for the entity to perform its duties and responsibilities; and, if disclosing to a contractor or subcontractor, prior to such disclosure, the governmental entity must first receive from the contractor or subcontractor a copy of the contractor's or subcontractor's policy that sets forth how

the requirements imposed under this Act on a governmental entity to protect an individual's social security number will be achieved.

2. The disclosure of social security numbers pursuant to a court order, warrant, or subpoena.
3. The collection, use, or disclosure of social security numbers in order to ensure the safety of: State and local government employees; persons committed to correctional facilities, local jails, and other law-enforcement facilities or retention centers; wards of the State; and all persons working in or visiting a State or local government agency facility.
4. The collection, use, or disclosure of social security numbers for internal verification or administrative purposes.
5. The disclosure of social security numbers by a State agency to any entity for the collection of delinquent child support or of any State debt or to a governmental agency to assist with an investigation or the prevention of fraud.
6. The collection or use of social security numbers to investigate or prevent fraud, to conduct background checks, to collect a debt, to obtain a credit report from a consumer reporting agency under the federal Fair Credit Reporting Act, to undertake any permissible purpose that is enumerated under the federal Gramm Leach Bliley Act, or to locate a missing person, a lost relative, or a person who is due a benefit, such as a pension benefit or an unclaimed property benefit.

VII. POLICY UPDATES

This Policy will be periodically reviewed and updated to try and reflect changes in risks to employees and customers and the soundness of the City from Identity Theft. At least once a year, the Policy Administrator will consider the City's experiences with Identity Theft, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, changes in types of accounts the City maintains and changes in the City's business arrangements with other entities. After considering these factors, the Policy Administrator will determine whether changes to the Policy, including the listing of Red Flags and internal practices, are warranted. If warranted, the Policy Administrator will update the Policy or present the Mayor and City Council with his or her recommended changes and the Mayor and City Council will make a determination of whether to accept, modify or reject those changes to the Policy.

VIII. POLICY ADMINISTRATION.

A. Oversight

Responsibility for developing, implementing and updating this Policy lies with the Identity Theft Committee. The Committee shall be headed by the Policy Administrator or his or her appointee. Two or more other individuals appointed by the City Council shall comprise the remainder of the committee membership. The Policy Administrator will be responsible for the Policy administration, for ensuring appropriate training of City staff on the Policy, for reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating Identity Theft, determining which steps of prevention and mitigation should be taken in particular circumstances and considering periodic changes to the Policy.

B. Staff Training and Reports

City staff responsible for implementing the Policy shall be trained either by or under the direction of the Policy Administrator in the detection of Red Flags and Identity Protection Act, and the

responsive steps to be taken when a Red Flag or problem is detected. Further training shall also be provided on a yearly basis or as needed to address changes in the Policy.

C. Service Provider Arrangements

In the event the City engages a Service Provider to perform an activity in connection with one or more Covered Accounts, the City will take the following steps to ensure the Service Provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of Identity Theft.

1. Require, by contract, that Service Providers have such policies and procedures in place; and

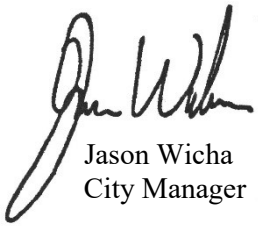
2. Require, by contract, that Service Providers review the City's Policy and report any Red Flags to the Policy Administrator.

D. Specific Policy Elements and Confidentiality

For the effectiveness of Identity Theft prevention policies, the Red Flag Rule envisions a degree of confidentiality regarding the City's specific practices relating to Identity Theft detection, prevention and mitigation. Therefore, under this Policy, knowledge of such specific practices is to be limited to the Identity Theft Committee and those employees who need to know them for purposes of preventing Identity Theft. Because this Policy is to be adopted by a public body and thus publicly available, it would be counterproductive to list these specific practices here. Therefore, only the Policy's general Red Flag detection, implementation and prevention practices are listed in this document.

IX. Distribution

This policy will be distributed to all employees who deal with personal identification information and published on the Human Resources website, www.citylf.org.



Jason Wicha
City Manager

Created 10-08
Revised 5-14, 5-19