5/23/2011

31-R-11

A RESOLUTION

ADOPTING THE CITY OF EVANSTON IDENTITY PROTECTION POLICY

WHEREAS, The Fair and Accurate Credit Transactions Act of 2003, Public Law 108-159, requires municipalities to promulgate rules regarding identity theft protection;

WHEREAS, on April 14, 2009, the City complied with the terms of the Act and adopted a resolution to establish the City's Identity Theft Prevention Program; and

WHEREAS, the Illinois Identity Protection Act, 5 ILCS 179/1 *et seq.* (the "Act") was enacted by the Illinois General Assembly and requires each local and state government agency to adopt an Identity Protection Policy; and

WHEREAS, The City of Evanston has determined that the following policy is in the best interest of the City and its citizens.

NOW, THEREFORE, BE IT RESOLVED BY THE CITY COUNCIL OF THE CITY OF EVANSTON, COOK COUNTY, ILLINOIS:

SECTION 1: The City of Evanston Identity Protection Policy, attached as Exhibit "A", is hereby adopted and approved.

SECTION 2: That this Resolution 31-R-11 shall be in full force and effect from and after its passage and approval in the manner provided by law.

Elizabeth B. Tisdahl, Mayor

Attest:

Rodney Greene, City Clerk

Adopted: June 13, 2011

EXHIBIT A

CITY OF EVANSTON IDENTITY THEFT POLICY

SECTION 1: BACKGROUND

The risk to the City of Evanston, its employees and customers from data loss and identity theft is of significant concern to the City and can be reduced only through the combined efforts of every employee and contractor.

SECTION 2: PURPOSE

The City of Evanston adopts this sensitive information policy to help protect employees, customers, contractors and the City from damages related to the loss or misuse of sensitive information.

This policy will:

1. Define sensitive information, with an emphasis on social security numbers;
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.

This policy enables the City to protect existing customers, reducing risk from identity fraud, and minimize potential damage to the City from fraudulent new accounts. The program will help the City of Evanston:

1. Identify risks that signify potentially fraudulent activity within new or existing covered accounts;
2. Detect risks when they occur in covered accounts;
3. Respond to risks to determine if fraudulent activity has occurred and act if fraud has been attempted or committed; and
4. Update the program periodically, including reviewing the accounts that are covered and the identified risks that are part of the program.

SECTION 3: SCOPE

This policy and protection program applies to employees, contractors, consultants, temporary workers, and other workers at the City, including all personnel affiliated with third parties.

SECTION 4: POLICY

4.A: Sensitive Information Policy

City personnel are encouraged to use common sense judgment in securing confidential information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their supervisor.

Definition of Sensitive Information - Sensitive information includes the following items whether stored in electronic or printed format:

Credit card information, including any of the following:

- Credit card number (in part or whole)
- Credit card expiration date
- Cardholder name
- Cardholder address

Tax identification numbers, including:

- Social Security number (see 4.B)
- Business identification number
- Employer identification numbers

Payroll information, including, among other information:

- Paychecks
- Pay stubs

Cafeteria plan check requests and associated paperwork

Medical information for any employee or customer, including but not limited to:

- Doctor names and claims
- Insurance claims
- Prescriptions
- Any related personal medical information

Other personal information belonging to any customer, employee or contractor, examples of which include:

- Date of birth
- Address
- Phone numbers
- Maiden name
- Names
- Customer number

4.B: Social Security Numbers

Social Security numbers are confidential and protected by state and federal law, including the Privacy Act of 1974 (5 USC §552a) and the Illinois Identity Protection Act. The Social Security number will be collected by The City of Evanston only when allowed by law. Except when allowed by law, individuals will not be asked to provide their social security number, verbally or in writing, at any point of service. However, individuals may volunteer their social security number if they wish as an alternate means of locating a record. The social security number will not be disclosed to individuals or agencies outside the City except as allowed or required by state or federal law, rules or regulations, or with permission from the individual. Social security numbers requested from an individual should be provided in a manner that makes the number easily redacted if required to be released as part of a public record request.

The Social Security number will be requested from all employees, in order to comply with the requirement of the Internal Revenue Service to supply them with the name, address, and social security number of every employee. The City is required to report income along with social security numbers for all employees to whom compensation is paid. Therefore, each employee, with specific exceptions as required by law, will be required to supply the City with a social security number for payroll, reporting and benefits purposes. Individuals who are affiliates or vendors will be required to provide a Social Security number or Tax Identification Number for mandated tax reporting purposes. Social security numbers will be requested from utility customers of the City in order to assist in the collection of delinquent debts. The utility customer may decline to provide the social security number. Utility customers of the City shall not be required to provide social security numbers to receive utility service.

If the collection of Social Security Numbers is required, a statement must first be provided to the individual explaining the purpose or purposes for which the City is collecting and using the social security number.

All records containing Social Security numbers, whether on- or off-line, in electronic or physical format, are considered confidential information and will be maintained appropriately. Any documents containing social security numbers must be redacted if required to be released as part of a public records request. Therefore, any social security numbers requested from an individual should be placed on the document in a manner that makes it easily redacted. If and when these records are no longer needed, disposal of the records must be handled in a secure fashion and follow the City's Record Retention Policy.

Only City employees required to use or handle information or documents containing social security numbers will have access to such information or documents. Those employees will be trained on the proper procedures for handling information containing social security numbers from the time of collection through the destruction of the information, in order to protect the confidentiality of social security numbers.

Pursuant to state law, social security numbers MAY NOT:

- Be publicly posted or displayed in any manner
- Be used as the employee ID or process or record key in any City systems.
- Be printed on any card required for the individual to access products or services provided by the City
- Be required to be transmitted over the Internet, unless the connection is secure or the social security number is encrypted
- Be printed on any materials that are mailed, e-mailed or otherwise delivered to the individual, unless State or federal law requires the social security number

to be on the document. EXCEPTION: Social security numbers may be included in applications and forms sent by mail, including, but not limited to, any material mailed in connection with 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. However, no social security number may be printed on a postcard or other mailer that does not require an envelope or is visible on an envelope without the envelope having been opened.

- Be used for any purpose other than the purpose for which it was collected
- Be required for an individual to access any City Internet or Intranet website

This policy does not preclude City employees from using a social security number as needed to perform their duties and responsibilities or for internal verification or administrative purposes.

An employee who has substantially breached the confidentiality of social security numbers may be subject to disciplinary action up to and including discharge or dismissal in accordance with City policies and procedures.

4.C: Hard Copy Distribution

Each employee and contractor performing work for the City will comply with the following policies:

1. File cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with sensitive information will be locked when not in use.
2. Storage rooms containing documents with sensitive information and record retention areas will be locked at the end of each workday or when unsupervised.
3. Desks, workstations, work areas, printers and fax machines, and common shared work areas will be cleared of all documents containing sensitive information when not in use.
4. Whiteboards, dry-erase boards, writing tablets, etc. in common shared work areas will be erased, removed, or shredded when not in use.
5. When documents containing sensitive information are discarded they will be placed inside a locked shred bin or immediately shredded using a mechanical cross cut or Department of Defense (DOD)-approved shredding device. Locked shred bins are labeled "*Confidential paper shredding and recycling.*" Municipal records, however, may only be destroyed in accordance with the city's records retention policy.

4.D: Electronic Distribution

Each employee and contractor performing work for the City will comply with the following policies:

1. Internally, sensitive information may be transmitted using approved municipal e-mail. All sensitive information must be encrypted when stored in an electronic format.
2. Any sensitive information sent externally must be encrypted and password protected and only to approved recipients. Additionally, a statement such as this should be included in the e-mail:

   "This message may contain 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."

SECTION 5: ADDITIONAL IDENTITY THEFT PREVENTION PROGRAM

5.A: Covered accounts

A covered account includes any account that involves or is designed to permit multiple payments or transactions. Every new and existing customer account that meets the following criteria is covered by this program:

1. Business, personal and household accounts for which there is a reasonably foreseeable risk of identity theft; or
2. Business, personal and household accounts for which there is a reasonably foreseeable risk to the safety or soundness of the City from identity theft, including financial, operational, compliance, reputation, or litigation risks.

5.B: Red flags

The following red flags are potential indicators of fraud. Any time a red flag, or a situation closely resembling a red flag, is apparent, it should be investigated for verification.

- Alerts, notifications or warnings from a consumer reporting agency;
- A fraud or active duty alert included with a consumer report;
- A notice of credit freeze from a consumer reporting agency in response to a request for a consumer report; or
- A notice of address discrepancy from a consumer reporting agency as defined in § 334.82(b) of the Fairness and Accuracy in Credit Transactions Act.

Red flags also include consumer reports that indicate a pattern of activity inconsistent with the history and usual pattern of activity of an applicant or customer, such 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 credit, especially with respect to recently established credit relationships; or
- An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

5.C: Suspicious documents

- 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 covered account or customer presenting the identification.
- Other information on the identification is not consistent with readily accessible information that is on file with the City, such as a signature card or a recent check.
- An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

5.D: Suspicious personal identifying information

Personal identifying information provided is inconsistent when compared against external information sources used by the City. For example:

- The address does not match any address in the consumer report;
- The Social Security number (SSN) has not been issued or is listed on the Social Security Administration's Death Master File; or
- Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.

Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the City. For example, the address on an application is the same as the address 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 used by the City. For example:

- The address on an application is fictitious, a mail drop, or a prison; or
- The phone number is invalid or is associated with a pager or answering service.

The SSN provided is the same as that submitted by other persons opening an account or other customers.

The address or telephone number provided is the same as or similar to the address or telephone number submitted by an unusually large number of other customers or other persons opening accounts.

The customer or the person opening the covered 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 personal identifying information that is on file with the City.

When using security questions (mother's maiden name, pet's name, etc.), the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

5.E: Unusual use of, or suspicious activity related to, the covered account

- Shortly following the notice of a change of address for a covered account, the City receives a request for new, additional, or replacement goods or services, or for the addition of authorized users on the account.

- A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example, the customer fails to make the first payment or makes an initial payment but no subsequent payments

- A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:
    - Nonpayment when there is no history of late or missed payments;
    - A material change in purchasing or usage patterns

- A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).

- 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 paper account statements.

- The City is notified of unauthorized charges or transactions in connection with a customer's covered account.

- The City receives notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the City.

- The City is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

SECTION 6: RESPONDING TO RED FLAGS

6.A: Once potentially fraudulent activity is detected, an employee must act quickly as a rapid appropriate response can protect customers and the City from damages and loss.

- Once potentially fraudulent activity is detected, gather all related documentation and write a description of the situation. Present this information to the designated authority for determination.
- The designated authority will complete additional authentication to determine whether the attempted transaction was fraudulent or authentic.

6.B: If a transaction is determined to be fraudulent, appropriate actions must be taken immediately. Actions may include:

- Canceling the transaction;
- Notifying and cooperating with appropriate law enforcement;
- Determining the extent of liability of the City; and
- Notifying the actual customer that fraud has been attempted.

SECTION 7: PERIODIC UPDATES TO PLAN

At periodic intervals established in the program, or as required, the program will be re-evaluated to determine whether all aspects of the program are up to date and applicable in the current business environment. Periodic reviews will include an assessment of which accounts are covered by the program. As part of the review, red flags may be revised, replaced or eliminated. Defining new red flags may also be appropriate.

Actions to take in the event that fraudulent activity is discovered may also require revision to reduce damage to the City and its customers.

SECTION 8: PROGRAM ADMINISTRATION

8.A: Involvement of management

1. The Identity Theft Prevention Program shall not be operated as an extension to existing fraud prevention programs, and its importance warrants the highest level of attention.
2. The Identity Theft Prevention Program is the responsibility of the governing body. Approval of the initial plan must be appropriately documented and maintained.

3. Operational responsibility of the program is delegated to the Department of Administrative Services.

8.B: Staff training

1. Staff training shall be conducted for all employees, officials and contractors for whom it is reasonably foreseeable that they may come into contact with accounts or personally identifiable information that may constitute a risk to the City or its customers.
2. The Department of Administrative Services is responsible for ensuring identity theft training for all requisite employees and contractors.
3. Applicable City employees should receive an initial training in all elements of this policy and additional training as changes to the program are implemented by the Corporate Authorities.

8.C: Oversight of service provider arrangements

1. It is the responsibility of the City to ensure that the activities of all service providers are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.
2. A service provider that maintains its own identity theft prevention program, consistent with the guidance of the red flag rules and validated by appropriate due diligence, may be considered to be meeting these requirements.
3. Any specific requirements should be specifically addressed in the appropriate contract arrangements.