4/14/2009

9-R-09

A RESOLUTION

Establishing the City's Identity Theft Prevention Program

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

SECTION 1: That the City of Evanston hereby adopts the Identity Theft Prevention Program, a copy of which is attached hereto as Exhibit A and incorporated herein by reference.

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

Lorraine H. Morton

Lorraine H. Morton, Mayor

Attest:

Rodney Greene

Rodney Greene, City Clerk

Adopted: April 14, 2009

EXHIBIT A

Identity Theft Prevention Program

City of Evanston
Identity Theft Prevention Program

Introduction and Background

On November 9, 2007, the Federal Trade Commission (FTC) and several other Federal agencies published the Identity Theft Red Flag Rule for Covered Accounts and require a program to comply with this rule by November 1, 2008. The deadline for compliance was later extended to May 1, 2009.

The Identity Theft Red Flag Rule requires any creditor to develop a program to detect, prevent, and mitigate identity theft. Utility companies are specifically mentioned in the definition of a creditor, so this Rule directly applies to the City of Evanston's water utility accounts as well as all other "covered accounts". A "red flag" is defined as a pattern, practice, or specific activity that indicates the possible existence of identity theft. "Identity theft" is defined as a fraud committed or attempted by using the identifying information of another person without authority. A "covered account" is defined as any account the City offers or maintains that involves multiple payments or transactions or for which there is a reasonably foreseeable identity theft risk to customers.

Part I. Assessment of Existing Business Practices

A. The City of Evanston provides customer service personnel with the ability to request and review a customer's personal identifying information when engaging in any of the following activities:

- Open new accounts;
- Access existing accounts;
- Modify existing accounts; and/or
- Close existing accounts.

B. The City of Evanston provides customers with the ability to do one or more of the following actions independent of Customer Service personnel through an online service know as eBilling. A customer's personal identifying information is required to complete any of these activities:

- Open a new account;
- Access an existing account;
- Modify an existing account; and/or
- Close an existing account.

The City of Evanston, to date, has experienced no known occurrences or attempts in terms of identity theft with regards to information collected for establishing, monitoring or closing a covered account. The Rule that was published in the *Federal Register* focuses to a great degree on Social Security Numbers. **The City of Evanston does not collect, store**

or maintain Social Security Numbers for any covered account activity whatsoever. Although not specifically required as part of an Identity Theft Program, the City of Evanston currently utilizes many guidelines in the protection of personal information. The divisions of Facilities Management, Business Performance and Technology (BPAT) work in conjunction with all City Departments in terms of document retention and destruction. These procedures include, but are not limited to the following:

1. Checking references or doing background checks before hiring employees who will have access to customer information.

2. Limiting access to customer information to employees who have a business reason to view or edit this information, but only to the extent they need it to do their jobs.

3. The City controls access to sensitive information by requiring employees to use passwords that must be changed on a regular basis.

4. Employees undergo training to take basic steps to maintain the security, confidentiality, and integrity of customer information, including:
a. Locking rooms and file cabinets where records are kept;
b. Discourage sharing or openly posting employee passwords in work areas;
c. Encrypting sensitive customer information when it is transmitted electronically via public networks;
d. Referring calls or other requests for customer information to designated individuals who have been trained in to safeguard personal data;
e. Reporting suspicious attempts to obtain customer information to designated personnel.

5. All employees are regularly reminded of the City's policy and the legal requirement to keep customer information secure and confidential as part of the ongoing training regarding the Identity Theft Prevention Program.

6. Disciplinary measures for security policy violations are utilized when appropriate.

7. Terminated employees are prevented from accessing customer information by immediately deactivating their passwords and user names and taking other appropriate measures.

8. Sensitive customer information is stored securely. Only authorized employees have access. For example:
a. Storage areas are protected against destruction or damage from physical hazards, like fire or floods.
b. Records are stored in a room or cabinet that is locked when unattended.
c. Customer information stored on a server or computer is accessible only with a "strong" password and servers are kept in a physically secure area.

9. The City takes steps to ensure the secure transmission of customer information. For example:

a. When transmitting credit card information or other sensitive financial data, The City uses a Secure Sockets Layer (SSL) or other secure connection, so that the information is protected in transit.
b. All online information collected directly from customers utilizes a secure transmission technology. Staff cautions customers against transmitting sensitive data, like account numbers, etc. via email or in response to an unsolicited email or pop-up messages.
c. When sensitive data is transmitted over the Internet, the data is encrypted.

10. The City disposes of customer information in a secure way and, where applicable, consistent with the FTC's Disposal Rule. These guidelines are adhered to and include but are not limited to the following:
a. Facilities Management staff supervise the disposal of records containing customer information.
b. A document destruction shredding company is utilized on site and under City supervision to shred documents containing customer information so that the information cannot be read or reconstructed.
c. When disposing of computers, disks, CDs, magnetic tapes, hard drives, laptops, PDAs, cell phones, hardware or any other electronic media containing customer information these items either are destroyed or have the memory erased.

11. The City monitors and reads relevant industry publications for news about emerging threats and available defenses.

12. The City maintains up-to-date and appropriate programs and controls to prevent unauthorized access to customer information. This includes the use of anti-virus and anti-spyware software that updates automatically, the maintenance of an up to date firewall system.

13. The City uses appropriate oversight or audit procedures to detect the improper disclosure or theft of customer information. This includes:
a. Keeping logs of activity on the network and monitoring them for signs of unauthorized access to customer information;
b. The use of an intrusion detection system to alert the City of electronic attacks;

14. The City takes many steps to preserve the security, confidentiality, and integrity of customer information in the event of a breach. If a breach occurs:
a. The City would take immediate action to secure any information that has or may have been compromised.
b. The City preserves and reviews files or programs that may reveal how the breach occurred;
c. When feasible and appropriate, Staff would bring in security professionals to help assess the breach as soon as possible.

15. After assessing the nature of a breach, the City would follow guidelines under applicable state law notifying consumers, law enforcement, and/or businesses in the event of a security breach. For example:

a. Consumers would be notified if their personal information has been subject to a breach that poses a significant risk of identity theft or related harm;
b. Law enforcement entities would be notified immediately if evidence that the breach resulted in identity theft or related harm.

Part II. Identification of Red Flags

Part II of the Identity Theft Prevention Program is designed to assist the City of Evanston in identifying Red Flags that may arise during routine handling of covered new and/or existing accounts. The City has identified the following items as potential Red Flag sources or categories that might indicate an instance of identity theft.

- Consumer report includes a fraud or active duty alert, a notice of credit freeze and/or a notice of address discrepancy.
- Documents provided for identification appear to have been altered or forged.
- Photograph, physical description and/or other information on the identification is not consistent with the appearance of the person presenting the identification.
- Information on the identification is not consistent with readily accessible information that is on file with the City.
- Information provided is inconsistent when compared against external information sources.
- Information provided is associated with known fraudulent activity (address and/or phone number on an application is the same as the address provided on a previous fraudulent application).
- Information provided is of a type commonly associated with fraudulent activity (address on an application is fictitious and/or phone number is invalid).
- Customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.
- Customer cannot provide authenticating information beyond that which generally would be available from a wallet.
- Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's account
- City is notified that the customer is not receiving paper account statements.
- City is notified that it has opened a fraudulent account for a person engaged in identity theft.

Part III. Detection of Red Flags & Sensitive Information

A. Red Flag Detection

Part III of the Identity Theft Prevention Program addresses the process of detecting Red Flags as related to possible identity theft during the City's routine handling of covered new and/or existing accounts. The following is a list of detection methods that the City uses to prevent identity theft.

1. Require customers to present information to open a new account. Types of necessary information include:

- Name
- Date of birth
- Address
- Phone number

2. Verify personal identification information using records on file with the City.
3. Independently contact the customer (in the case of phone or internet setup of new covered accounts).
4. When fielding a request to access and/or modify an existing account (such as a change of billing address), verify identity of customer by requesting specific pieces of personal identifying information (identification with the new billing address and/or documentation proving shift of financial liability).
5. If new banking information is provided for electronic payment of accounts, cross-check ownership of the new bank account with the customer name on the city account by contacting the appropriate financial institution.
6. For online or automated phone system access of covered account, require the establishment of security questions during the initial set-up of the account.

B. Sensitive Information Policy

Definition of sensitive information: sensitive information includes the following items whether stored in electronic or printed format which could be used on its own or in conjunction with other information to commit identity theft:

1.Credit card information, including any of the following:
   a. Credit card number (in whole or part)
   b. Credit card expiration date
   c. Cardholder name
   d. Cardholder address

2. Other personal information belonging to any customer, employee or contractor, examples of which include:
   a. Names
   b. Address
   c. Phone numbers
   d. Date of birth
   e. Customer account number

City personnel are expected to use the utmost of care in securing sensitive information. Furthermore, this section should be read in conjunction with the Illinois Local Records Act, the City's information technology policies and guidelines and the City's local records

policy. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact his/her supervisor.

Part IV. Prevention and Mitigation

Part IV of the Identity Theft Prevention Program details response actions for the City of Evanston personnel if the personnel have observed a Red Flag associated with a new or existing covered account. One or more of the following actions will be taken by the City to rectify the situation.

1. Staff will not open a new account (after review of the identifying information and discussion with department supervisor).
2. For an existing account, the City may discontinue the services associated with that account and/or:

- Continue to monitor the account for evidence of identity theft and contact the customer to discuss possible actions.
- Change the passwords, security codes, or other security devices that permit access to an existing account.
- Reopen an existing account with a new account number.
- Close an existing account.

3. Should the City identify an instance of identity theft associated with an unpaid account, there will be no attempt to collect on the account or sell the account to a debt collector.
4. If applicable, the City will provide the consumer reporting agencies with a description of the identity theft event.
5. For all instances of suspected or confirmed identity theft, Staff will notify local law enforcement and will provide them with all the relevant details associated with the identity theft event.

Part V. Program Administration

Program administration is an important part of the Identity Theft Prevention Program. This section details the training requirements, annual program review, approval and adoption process and annual reporting requirements that are associated with the Program.

A. Staff Training

Any employee with the ability to open a new account, or access/manage/close an existing account will receive training on identifying and detecting Red Flags. They will also be trained in the appropriate response actions in the event that an instance of identity theft is suspected. Key management and customer service personnel in appropriate departments will also receive training on the contents of this Program. As necessary, employees will be re-trained annually if the Program is updated to include new methods of identifying and detecting Red Flags, or if new response actions are implemented. Each employee must sign the City's designated form after Red Flag training has been received.

B. Program Review and Update

The City will review and update the Program annually to reflect changes in risks to customers from identity theft based on factors such as:

- Experiences of the City with identity theft.
- Changes in methods of identity theft.
- Changes in methods to detect, prevent, and mitigate identity theft.
- Changes in the types of accounts that the City offers or maintains.
- Changes in the business arrangements of the City, including alliances, joint ventures, and service provider arrangements.

C. Program Approval and Adoption

This Program has been reviewed and approved by the Evanston City Council on March 23, 2009. The City Manager's Office will be responsible for the oversight, development, implementation and administration of the Program. An annual report as described in Section D below that will address compliance of the City of Evanston with this Program will be submitted to the City Council for review and approval of any changes recommended by Staff.

D. Annual Reporting

City of Evanston staff will provide an annual report to the Evanston City Council that details compliance with the Federal Trade Commission's Red Flags Rule. The report will address matters related to the Program and address several topic areas including:

- Effectiveness of the policies and procedures in addressing the risk of identity theft in connection with the opening of new accounts and with respect to the management of existing accounts;
- Service provider arrangements;
- Significant incidents involving identity theft and management's response; and,
- Recommendations for material changes to the Program.

E. Service Provider Oversight

Currently, the City of Evanston engages several service providers to perform activities in connection with one or more customer accounts. Staff will verify that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. To accomplish this, staff will require the service provider by contract to have policies and procedures to detect relevant Red Flags that may arise in the performance of the service provider's activities, and either report the Red Flags to the City, or to take appropriate steps to prevent or mitigate identity theft.

Part VI. Evanston Covered Account Procedures and Customer Information

The promulgation and implementation of Identity Theft Prevention Programs like that of the City of Evanston as outlined above illuminate the growing concern regarding identity theft. Unfortunately, it is a problem that is not easily resolved. There are several ways to protect your personal information with regards to your Evanston covered account:

1. The easiest and most efficient way is to place a password on your City of Evanston covered account. Currently, when utilizing the internet eBilling system, you must first set up a user id and a unique password. This can also be done with regards to any exchange of information by telephone with an Evanston Customer Service Representative by calling (847) 328-2100 and requesting this service.
2. Verify the authenticity of any City of Evanston Customer Service Representative if you receive a call requesting any additional personal information. Please ask for the person's name and call the City of Evanston main switchboard at 847-328-2100 and ask to be connected to this individual.
3. If you feel that your personal information has been compromised due to your Evanston covered account information, please contact one of our Customer Service Representatives by call (847) 328-2100. Staff will verify your account information and make sure it is consistent with our records. If we discover suspicious charges, we will investigate these charges to the full extent of the law.

The City of Evanston is committed to providing outstanding customer service and take the threat of identify theft very seriously. A copy of the entire Identity Theft Prevention Policy can be obtained by contacting the Evanston at (847) 328-2100 and requesting to speak with an employee in the City Manager's Office. If you have access to the internet, please visit our website at www.cityofevanston.org where a link to the policy may be found.