

RESOLUTION #887

A RESOLUTION OF THE CITY COUNCIL OF THE CITY OF LAKE WORTH, TEXAS, ADOPTING A WRITTEN IDENTITY THEFT PROGRAM POLICY AND AUTHORIZING THE CITY MANAGER TO APPROVE CHANGES IN THE POLICY.

WHEREAS, the Federal Trade Commission (FTC) recently adopted rules on identity theft “red flags”, or warning signs, pursuant to the Fair and Accurate Credit Transactions (FACT) Act of 2003; and

WHEREAS, the new rules, which require action by November 1, 2008, require any business with a “covered account” to adopt and implement an identity theft program; and

WHEREAS, a “covered account” is one where an entity, such as a municipal water utility, provides a service or good before the consumer pays for it; and

WHEREAS, a city with such accounts must adopt a program by November 1, 2008 that “red flags” relevant identity theft, provides detection of the “red flags”, provides appropriate responses for any “red flags” detected, and ensures the program is updated periodically to address changing risks; and

WHEREAS, the City of Lake Worth services such water utility customers and, therefore, falls within this federal mandate; and


WHEREAS, the City Council of the City of Lake Worth wishes to be proactive and adopt an Identity Theft Program Policy that will be in compliance with the criteria set forth by the FTC.

NOW, THEREFORE, BE IT RESOLVED BY THE CITY COUNCIL OF THE CITY OF LAKE WORTH to adopt the Identity Theft Program Policy that is in compliance with federal law and is attached to this resolution as Exhibit “A”. This resolution shall be effective immediately upon its adoption on this 14th day of October, 2008.

Approved:


Walter Bowen, Mayor

Attest:


Linda Rhodes, TRMC/CMC
City Secretary

CITY OF LAKE WORTH, TEXAS
Identity Theft Program/Policy
“Red Flags Rules”

I. Purpose

To ensure the City of Lake Worth has a program in place to identify, detect, prevent, diminish, and respond to identity theft in connection with the opening of water accounts, and to establish written procedures for security and storing of personal information, pursuant to the Identity Theft Red Flags Regulation implemented pursuant to Section 114 of the Fair and Accurate Credit Transactions (FACT) Act of 2008, to be effective on November 1, 2008.

II. Application

This policy applies to all City employees and service providers that have access to personal information for customers of the Utility Billing Department, regardless of medium.

III. Definitions

Identity Theft: A fraud committed using the identifying information of another person.

Red Flags: A pattern, practice, or specific activity that indicates the possible risk of identity theft.

Identifying Information: Any name or number that may be used alone or with any other information to identify a specific person (includes name, social security number, date of birth, alien registration number, government passport, and employer/tax identification number).

IV. Policy

A. Red Flags Alerts

When opening new accounts, staff needs to carefully scrutinize documents submitted for identification or proof of residency for red flags such as:

1. Documents provided for identification appear to be altered or forged.
2. The photograph or physical description on the identification is not consistent with the appearance of the customer requesting service.
3. Other information on the identification is not consistent with information provided by the person requesting service.
4. Other information is not consistent with information that is on file (i.e. previous application submitted with driver's license).

5. Lease or deed submitted for proof of residency appears to be altered or forged.
6. Personal information submitted is associated with known fraudulent activity.
7. The social security number submitted is the same as another customer's.
8. Notification of a chargeback received from the bank.
9. New account requested immediately after disconnection for non-payment.

B. New Account Activation

1. To ensure proper identification verification, effective November 1, 2008, all requests for new service must be completed in person.
2. Applicants must show a government issued photo ID (or two forms of picture identification) in person to initiate service.
3. Applications may be submitted by fax, e-mail, or mail, but will not be processed until proper identification verification is completed in person.
4. Applications must be completed by the person seeking to open an account. The name on the application must match the submitted identification and lease agreement/deed.
5. The City reserves the right to refuse service in the event of inability to provide sufficient identification.

C. Credit Card Transactions

The City accepts credit card payments via service vendor Official Payments. Customers paying with a credit card in person must show valid identification that matches the name and/or address on the credit card.

D. Data Security and Storage

1. Employees are required to maintain a high level of confidentiality as it relates to utility customer's personal information. Release of information is limited to the account holder(s) or as permitted by law. Customers are given the opportunity to indicate if they wish their account information to be kept confidential.
2. Access into the billing system requires a user name assigned by the System Administrator. A password is also required, which is determined by the user and is CJIS (Criminal Justice Information Systems) compliant based upon the City's IT Security Policy that has been implemented. The system will permit three (3) sign on attempts and then will temporarily disable the password. Upon termination, employee passwords are immediately disabled.
3. Disclosure of personal information. Personal information is, or could be, used as a means of identification, for internal verification, or administration purposes, credit checks, and for debt collection purposes. Information submitted to the city's debt collection agency is on file in the Utility Billing office.
4. Data Storage. Hard copy information is stored in filing cabinets in the Utility Billing Office. The office is monitored by security cameras and

two (2) locked doors. Cash receipt information is stored in the locked safe and the Senior Accountants storage areas.

E. Data Retention/Access

Records are disposed of in accordance with state and federal law including the local records retention schedule issued by the Texas State Library and Archives Commission and City Code.

All City records are subject to the Texas Public Information Act. Requests for information that falls within confidentiality conditions are forwarded to the Attorney General's office for an official ruling for the information to be withheld.

F. Identity Theft Notification

A zero tolerance policy is in effect for all fraudulent transactions pertaining to the Utility Billing Department. Once written notification and verification is received of fraudulent activity from a customer, banking institution, and/or collection agency, the Utility Billing Department will (1) proceed with notating and taking corrective actions on the account, (2) gather all pertinent information that is available, and (3) immediately contact the City of Lake Worth Police Department to initiate a criminal investigation.

G. Periodic Review and Reporting

The Finance Director will conduct an annual review of the current policy and report any fraudulent activity to the City Manager. The City Manager will approve any recommended changes in policy.