CITY OF SPRINGFIELD, FLORIDA
BAY COUNTY, FLORIDA
RESOLUTION NO.: 08-11

A RESOLUTION OF THE CITY OF SPRINGFIELD, FLORIDA, IN BAY COUNTY, FLORIDA; ADOPTING AN IDENTITY THEFT PREVENTION POLICY; IMPLEMENTING EMPLOYEE TRAINING PROCEDURES FOR THE IDENTITY THEFT PREVENTION POLICY; REQUIRING AN ANNUAL REVIEW AND APPROVAL OF THE IDENTITY THEFT PREVENTION POLICY WITH OR WITHOUT ANY CHANGES; AND PROVIDING FOR AN EFFECTIVE DATE.

WHEREAS, the City of Springfield is required by the Federal Trade Commission (FTC) to implement and adopt an Identity Theft Prevention Policy on or before November 1st, 2008; and

WHEREAS, the first objective of the City's Identity Theft Prevention Policy is to protect sensitive and non-public information of its customers, employees and contractors; and

WHEREAS, the City Commission and the employees of the City of Springfield have a responsibility to prevent the establishment of false accounts and ensure existing accounts are not being manipulated; and

WHEREAS, the City Commission recognizes the importance of implementing employee training procedures for the Identity Theft Prevention Policy; and

WHEREAS, the City Commission also recognizes the value of an annual review and approval of the City's Identity Theft Prevention Policy.

NOW, THEREFORE, BE IT RESOLVED THE CITY OF SPRINGFIELD, FLORIDA AS FOLLOWS:

SECTION 1. The City Commission does hereby approve the Identity Theft Prevention Policy (Attachment A) and upon adoption hereof, the Policy shall be deemed adopted and in full force.

SECTION 2. The City Commission does hereby require an annual review of the Policy to assess any needed updates, make necessary changes, if any, and require the Policy with or without changes be adopted by this governing body on an annual basis.

SECTION 3. The City Commission does hereby authorize the City Clerk to implement procedures for all employees to receive continual training relevant to the protection of sensitive and non-public information and the prevention of the establishment of false accounts and manipulation of existing accounts pursuant to the City's Policy.

SECTION 4. This resolution shall take effect immediately upon its passage and adoption.

PASSED, APPROVED AND ADOPTED in special session of the City Commission of the City of Springfield, Bay County, Florida this 20TH day of October, 2008.

ATTEST:

Teresa Cox

Teresa Cox, City Clerk

CITY OF SPRINGFIELD, FLORIDA

Robert E. Walker

"Attachment A"

CITY OF SPRINGFIELD
IDENTITY THEFT PREVENTION POLICY

I. PURPOSE.

The City of Springfield adopts this policy to protect sensitive and non-public information of its customers, employees and contractors, prevent the establishment of false accounts and ensure existing accounts are not being manipulated, and to provide an affirmative defense to claims for damages related to loss or misuse of sensitive information. This policy will:

- Define sensitive information and other relevant terminology.
- Provide security procedures to protect sensitive and non-public information in all data formats including hard copy and electronic.
- Provide examples of ways to detect red flags.
- Identify procedures to prevent the establishment of false accounts.
- Identify procedures to prevent the manipulation of existing accounts.
- Define the roles and responsibilities of all employees.
- Provide for enforcement.

II. SCOPE.

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

III. DEFINITIONS.

Electronic Data. All data received, transmitted or stored electronically including but not limited to data on computers, cd's, jump drives, disks, email, laptops, etc. Electronic data is also considered to be *soft* data because it exists only electronically.

Encryption. The translation of data into a secret code requiring access by way of a secret key or password that enables you to decrypt or remove the code.

False Account. An account established using personal information that is either stolen, altered, inconsistent with other documentation, reassembled, misrepresented, created by an unauthorized source, considered to be fake or illegitimate, presented by someone other than the person it belongs to or otherwise presented falsely.

Hard Copy Data. All data received, transmitted or stored in a printed format including but not limited to paper, card files, whiteboards, dry-erase boards, etc.

Identity Theft. The criminal act of stealing personal information with the intent to use it to gain access to a person's identity for illegal purposes without the victim's knowledge.

Manipulated Account. An account that has been accessed, changed or altered in some way for any purpose of which the legitimate account owner has not authorized.

Non-Public Information.

- ***Other Personal Information*** - Exempt by Florida Statutes for specific customers, employees, and contractors which may include: date of birth, address, phone numbers, maiden name, customer number, or information relative to a qualified person(s) spouse and / or children or any other information that could otherwise identify certain person(s) whose personal information is protected by Florida Statutes.
- ***Confidential Information*** - any document or file marked "Confidential", "Sensitive", "Proprietary", or any document similarly labeled for the protection and security of the City as prescribed by law.

Personal Information. Information that is specific to only one person such as financial records, medical records, employment records, legal records, driving records, etc.

Red Flag. An indicator of fraudulent or potential fraudulent activity; an indicator of illegal action or use of personal information no belonging to the applicant or person(s) in question; an indicator of suspicious activity.

Sensitive Information. Consists of personal information, whether stored in electronic or printed format, including but not limited to the following:

- ***Credit Card Information*** - number (in part or whole), expiration date, cardholder name, cardholder address.
- ***Medical Information*** - doctors names and claims, insurance claims, prescriptions, any other related personal medical information.
- ***Tax Identification Information*** - social security number or social insurance number.

IV. SECURITY PROCEDURES.

All employees, consultants and contractors of the City will observe and follow the security procedures listed below when they are in contact with any information or data that is sensitive, non-public or that they may perceive to be sensitive or non-public, whether it is or not.

A. File cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with sensitive information will be locked when not in use.

B. Storage rooms containing documents with sensitive information and record retention areas will be locked at the end of each day. Only specifically identified employees with a legitimate need will have key(s) to room(s) and/or filing cabinets containing sensitive information.

C. 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.

D. 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. Any data storage media containing sensitive information will be disposed of by shredding, punching holes in it or incineration.

E. Internally, sensitive information may be transmitted using approved company email and all sensitive information must be encrypted when stored in an electronic format. Additionally, a statement such as this should be included in the email as follows: "*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.*"

F. Computer and network access will require a password and user names and passwords will be different. Passwords will not be shared or posted near workstations. Employees will log off of their work stations when leaving their work areas.

G. Any sensitive information sent externally must be encrypted and password protected and sent only to approved recipients. Any sensitive information shipped to an external entity, will be shipped using a shipping service that allows tracking of the delivery of the information.

H. Visitors who must enter areas where sensitive files are kept must be escorted by an employee at all times while in these areas. No visitor will be given any entry codes or allowed unescorted access to the office or any area containing or that might contain sensitive information.

I. The use of laptops is restricted to those employees who need them to perform their jobs. Laptops which contain sensitive data will be encrypted and password protected. Laptops are to be stored in a secure place at all times. Employees are prohibited from leaving laptops containing sensitive information at a hotel luggage stand or packed in checked luggage and should take extra measures to secure any vehicle containing a laptop with sensitive information on it.

J. Installation of software, new or otherwise, will be installed by the City's IT Consultant only. Downloads of materials not related to the performance of an employees duties or coming from an unauthorized source are prohibited.

All employees and contractors of the City are encouraged to use common sense judgment in securing sensitive or non-public information. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their immediate supervisor.

V. IDENTIFYING RED FLAGS (Detecting Fraudulent Activity).

The City of Springfield acknowledges the *Red Flags* listed below to detect fraudulent or potentially fraudulent activity. These are not intended to be all-inclusive and other suspicious activity may be investigated as necessary.

A. Identification documents appear to be altered.
B. Photo and physical description do not match appearance of applicant.
C. Information provided by applicant is inconsistent with information on file.
D. Personal information provided by application does not match other sources of information (e.g. credit reports, SS# not issued or listed as deceased).
E. Lack of correlation between social security number range and date of birth.
F. Information provided is associated with known fraudulent activity (e.g. address or phone number provided is same as that of a fraudulent application).
G. Information commonly associated with fraudulent activity is provided by applicant (e.g. address that is a mail drop or prison, non-working phone number or associated with answering service/pager).
H. SS#, address, or telephone numbers is the same as that of another customer.
I. Customer fails to provide all information requested.
J. Identity theft is reported or discovered.
K. A recent and significant increase in volume of inquiries.
L. Applicant has had numerous accounts closed for cause or abuse.

VI. PROCEDURES TO PREVENT THE ESTABLISHMENT OF A FALSE ACCOUNT AND THE MANIPULATION OF AN EXISTING ACCOUNT.

Any employee or contractor that may suspect fraud or detect a red flag will implement the following response as applicable.

- Ask the applicant for additional documentation.
- Notify immediate supervisor of suspicious activity or of detected red flag.
- Notify the Springfield Police Department of any attempted or actual identity theft.
- Do not open the account.
- Close the account.
- Do not attempt to collect against the account but provide the account information to the authorities.
- Do not give out sensitive or non-public information over the phone and do not ask for sensitive or non-public information over the phone.
- If the applicant is on the phone asking for sensitive information, try to obtain contact information for the applicant and provide this information to the authorities.
- All accounts that are opened are to be opened in person with required, verifiable and reliable documentation per City policy (e.g. a valid driver's

license or picture identification card, an authentic social security card and a copy of a lease or closing papers proving ownership of property).

- If an account has been turned off for non-payment, require documentation applicant was not on the prior tenant's lease and did not live at the residence during the time the service was provided.
- Document calls made by someone other than the name on the account. Be sure to include the name given, the type of information requested, the date and time the call was received each time.
- Ask for assistance from a supervisor if you are not sure whether or not part or all of the documentation may be valid.
- Do compare photos and signatures of applicants with those on the documentation provided.
- Ask the applicant to come in and talk with you about sensitive information that has been requested. Then alert your supervisor.
- Notify any suspicious activity or unauthorized changes in an account.

VII. ROLES AND RESPONSIBILITIES.

The City of Springfield acknowledges that employees and contractors at all levels are responsible in observing the guidelines established by this policy. Employees and contractors are expected to be diligent in protecting sensitive and non-public information. The following requirements are included but not limited by this policy:

A. Employees are prohibited from accessing sensitive or non-public information unless requested to do so by the person whose information is sensitive and provided that person has provided sufficient documentation in person or as required by an immediate supervisor.

B. Employees are required to notify their supervisor immediately of suspicious or fraudulent activity including but not limited to the detection of a red flag.

C. Supervisors are required to immediately report suspicious or fraudulent activity including but not limited to the detection of a red flag to the Springfield Police Department. In addition, the supervisor will provide all documentation available to assist in the investigation of such activity.

D.. Employees are required to be alert to attempts at phone phishing (requests for sensitive information without providing documentation) and reports such attempts to their supervisor.

E. New employees are required to sign an agreement to follow the security procedures listed in this policy.

F. Employees who will have access to sensitive data are required to have a background check and reliable references before they are hired.

G. Service providers are required to notify the City of any security incidents they

experience, even if the incidents may not have led to an actual compromise of the City's data.

H. Employees are required to monitor incoming and outgoing traffic for signs of a data breach.

I. Employees are prohibited from connecting to any unsecured wireless network on a City laptop.

J. Employees are required to notify the City Clerk immediately if there is a potential security breach, such as a lost or stolen laptop or lost keys.

K. Supervisors are required to report violations of this policy to the City Clerk and the City Mayor.

L. Supervisors are required to limit access to customer's personal identifying information to those employees who "need to know" only.

M. Supervisors are required to immediately report workers who leave the City's employment or transfer to another department and can no longer have access to sensitive information. This includes notifying the City's IT Consultant to disable all password and email access for those employees.

N. Supervisors are required to notify the City Clerk when a new employee is hired so initial Identity Theft Prevention training can be provided and to assist in the notification to employees to attend additional, annual training as provided.

O. As a condition of employment, all employees are required to take the Identity Theft Prevention Training within the first 30 days of employment and annually as it is provided by the City.

P. Supervisors are required to enforce this policy and ensure that it is followed by all employees and contractors.

VIII. ENFORCEMENT.

Any employee found to have violated any portion of this policy may be subject to disciplinary action, up to and including termination of employment.