RESOLUTION 20-60

A RESOLUTION TO APPROVE AN IDENTITY THEFT PREVENTION / SENSITIVE INFORMATION PROTECTION PROGRAM FOR THE CITY OF SPRING HILL

WHEREAS, the City of Spring Hill, in conjunction with providing essential utility services, collects certain information from its citizens/customers; and

WHEREAS, some of the information collected may be categorized as sensitive information that needs to be protected; and

WHEREAS, a written policy is required identifying the sensitive information held by the City and identifying items/situations that would be considered as "Red Flags" (a pattern, practice or activity that indicates the possible existence of identity theft); and

WHEREAS, the Program shall be reviewed and updated, if necessary, on an annual basis; and

WHEREAS, the Program shall be approved by the Board of Mayor and Aldermen and overseen by the Finance Director.

NOW THEREFORE, be it resolved by the City of Spring Hill, Tennessee that the Identity Theft Prevention / Sensitive Information Protection Program is hereby approved.

Passed and adopted by the Board of Mayor and Aldermen of the City of Spring Hill, Tennessee on the 15th day of June, 2020.

Rick Graham, Mayor

ATTEST:

April Goad, City Recorder

LEGAL FORM APPROVED:

Patrick Carter, City Attorney

City of Spring Hill

Board of Mayor and Aldermen

Date: May 15, 2020

Memo to: Board of Mayor and Aldermen

From: Patti Amorello, Finance Associate

Re: Identity Theft Prevention/Sensitive Information Protection Program

RESOLUTION NUMBER 20-60 A RESOLUTION TO APPROVE AN IDENTITY THEFT PREVENTION / SENSITIVE INFORMATION PROTECTION PROGRAM FOR THE CITY OF SPRING HILL

BACKGROUND INFORMATION: In order to operate and provide essential services to its residents/utility customers, the City of Spring Hill must collect certain information to establish customer accounts. Some of the data collected may contain "sensitive information" including driver's license numbers and bank account information.

A written program is required identifying the sensitive information held by the City and identifying items/situations that would be considered as "Red Flags" (patterns, practices or activities that indicate the possible existence of identity theft). Additionally, staff training is required to ensure that staff members are aware of both the sensitive information held and the appropriate processes for securing that information.

The development, adoption, implementation and ongoing management of this program are also prerequisites for the City to apply for privacy, network liability and cyber extension insurance coverage through Public Entity Partners (PEP) at the July 1st renewal date. Supplemental items including a completed application and a data breach recovery plan will be required in conjunction with applying for the coverage, which will be part of the City's liability insurance policy. The estimated cost of the additional insurance coverage is $7,500 annually. Annual invoices from PEP for the City's insurance policy renewals are presented to the Board of Mayor and Aldermen for approval prior to payment.

The program will be overseen by the Finance Director after approval from the Board of Mayor and Aldermen.

ATTACHMENTS: Resolution 20-60, A Resolution to Approve an Identity Theft Prevention/Sensitive Information Protection Program for the City of Spring Hill.

RECOMMENDATION: Approve Resolution 20-60.

IDENTITY THEFT PREVENTION/SENSITIVE INFORMATION PROTECTION PROGRAM
CITY OF SPRING HILL

The City of Spring Hill (the "City") provides water, sewer, stormwater and sanitation services to owners/tenants of property within the City's designated utility service areas. The City maintains accounts for these utility services, whereby each customer is billed in arrears on a monthly basis for water used and/or sewage treated. The City adopts this Identity Theft Prevention/Sensitive Information Protection Program (the "Program") designed to detect, prevent and mitigate identity theft in connection with the City's customer accounts. A "Red Flag" as used herein, is a pattern, practice or specific activity that indicates the possible existence of identity theft.

SECTION I. IDENTIFICATION OF RELEVANT RED FLAGS

A. **Risk Factors**. In identifying relevant Red Flags associated with customer accounts, the City's management and Board of Mayor and Aldermen have considered the following identity theft risk factors:

1. Types of Covered Accounts – The City opens and maintains customer accounts for persons to pay for utility services provided by the City. For each customer account, bills are sent and payments are due monthly in arrears.

2. Identifying Information Maintained. The City requires that persons or businesses which wish to receive utility service submit an application for utility service. The following information (hereinafter referred to as "identifying information") may be included on new and existing applications and/or other forms submitted by customers and on file with the City:

   (a) Name of adult household members on the account.
   (b) Telephone number.
   (c) Address location where service shall be provided.
   (d) Mailing address if different than service address.
   (e) Contact and billing information.
   (f) Driver's license number.
   (h) Employment information.
   (i) Bank account information (for those enrolled in automatic bank draft).

Such identifying information is not considered private under Tennessee state law, unless specifically designated as a private record. Under T.C.A. § 10-7-504, federal tax identification numbers, social security numbers and bank account information are designated as private records. Private records are to be treated as confidential and shall not be open for inspection by members of the public.

3. Methods for Accessing Accounts. The City allows customers to access information related to their accounts using the following methods:

(a) In person at the water and sewer business office,
(b) Over the telephone,
(c) Online through a link on the City's website (to make payments).

4. Previous Experience with Identity Theft. With the exception of the November 2017 cyberattack where the City was locked out of its computer systems (customer data was not taken), the City is not aware of any security breach of or unauthorized access to its system used to store customers' identifying information. The historical absence of such breaches of unauthorized access is due to (1) the limited services and credit provided to the City's customers, both of which are tied to an immovable physical location; (2) the size of the population the City serves; and (3) the relatively low rate of change in customer base.

B. **Sources of Red Flag Information.** In identifying relevant Red Flags associated with customer accounts, the City will consider the following sources of information:

1. Past Incidents of Identity Theft. As described in Section I.A.4. above, the City is not aware of any security breach of or unauthorized access to its system used to store customers' personal identifying information collected by the Water and Sewer Department. In the event of incidents of identity theft in the future, such incidents shall be used to identify additional Red Flags, and this Program will be amended accordingly.

2. Identified Changes in Methods of Identity Theft. The City will review methods of identity theft it has identified to assess changes in identity theft risks.

3. Applicable Regulatory Guidance. As a part of its annual review, the City will review additional regulatory guidance from the FTC and other consumer protection authorities on new identity theft risks and recommended practices for identifying, detecting, and preventing identity theft.

C. **Categories of Red Flags.** In identifying relevant Red Flags associated with customer accounts, the City will consider the following categories:

1. Suspicious Documents. The presentation of suspicious documents can be a Red Flag for identity theft. Examples of suspicious documents may include the following:

   (a) Documents provided for identification appear to have been altered or forged.
   (b) The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
   (c) Other information on the identification is not consistent with information provided by the person opening a new account or the customer presenting the identification.
   (d) Other information on the identification is not consistent with readily accessible information that is on file with the City, such as the customer's application for service.
   (e) An application for service appears to have been altered or forged or gives the appearance of having been destroyed and reassembled.

2. Suspicious Personal Identifying Information. The presentation of suspicious personal identifying information can be a Red Flag for identity theft. Presentation of suspicious personal identifying information may occur when:

(a) Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer.
(b) Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the City. For example:
(i) The address on an application for service is the same as the address provided on a fraudulent application; or
(ii) The phone number on an application is the same as the number provided on a fraudulent application.
(c) 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:
(i) The mailing address on an application is fictitious, or a mail drop; or
(ii) The phone number is invalid or is associated with a pager or answering service.
(d) The person opening the covered account or the customer fails to provide all required personal identifying information on an application for service or in response to notification that the application is incomplete.
(e) Personal identifying information provided is not consistent with personal identifying information that is on file with the City.

3. Suspicious Activity. The unusual use of or other suspicious activity related to a customer account can be a Red Flag for identity theft. Suspicious activities may include:

(a) A customer fails to make the first payment or makes an initial payment but no subsequent payments on the account.
(b) A customer account is used in a manner which is not consistent with established patterns of use on the account such as:
(i) Nonpayment when there is no history of late or missed payments; or
(ii) A material change in the amount of utility service purchased;
(c) Mail sent to the customer is returned repeatedly as undeliverable although utility purchases continue to be made on the customer account.
(d) A request is made, by a person claiming to be a customer or by another person, for a customer's confidential information from the City's records.

4. Notices. Notices of potential identity theft are serious Red Flags may include:

(a) Notices from customers, law enforcement authorities or other persons indicating that a customer or other person may have been a victim of identity theft.
(b) Notices to the City that a person has provided information to someone fraudulently claiming to represent the City.
(c) Notices to the City that a fraudulent website which appears similar to the City's website is being used to solicit customer personal identifying information.

(d) E-mails not initiated by the City, but returned on the City's mail servers, indicating that a customer may have received fraudulent e-mail soliciting customer personal identifying information.

SECTION II. DETECTING RED FLAGS

A. City personnel are encouraged to use common sense judgment in securing identifying The City shall obtain identifying information about a person opening a customer account and shall verify the identity of the person opening a customer account. The City will obtain the following information to open a customer account:

1. Name of adult household members on the account;
2. Address location where service shall be provided;
3. Mailing address if different than service address;
4. Contact and billing information;
5. Driver's license number, or other governmental identification information if no driver's license number is available; and
6. Employment information.

B. For existing customer accounts, the City shall monitor transactions and verify the validity of requests for change of address or other information.

SECTION III. PREVENTING AND MITIGATING IDENTIFY THEFT

A. City personnel are encouraged to use common sense judgment in securing identifying information to the proper extent. Furthermore, this section should be read in conjunction with the open records laws of the State of Tennessee. Identifying information will be considered a public record if it is not designated as a private record by law. Nonetheless, identifying information will be protected to the extent permitted by law, and will not be made available except as required by law. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact a supervisor. In the event that the City cannot resolve a conflict between this policy and state law, the City will contact the Tennessee Office of Open Records.

B. The City shall not provide information, either verbally, in writing or in electronic format, which is identified as confidential under the laws of the State of Tennessee, except under such circumstances as may be permitted by such laws.

C. Security of Electronic Records. The storage and transmission of customer account information shall be subject to the following policies:

1. Customer account information stored in electronic format shall be available only to those City employees for whom access is approved by the Finance Director. The Finance Director shall periodically review access provisions and procedures with the

City's Technology Department to determine that appropriate safeguards are in place to protect confidential information maintained in electronic format.

2. Access to all City servers will be controlled using "strong" passwords. Employees will choose passwords with a mix of letters, numbers, and characters. User names and passwords will be different. Passwords will not be shared or posted near workstations. Password-activated screen savers will be used to lock employee computers after a period of inactivity.
3. Customer account information shall not be downloaded or maintained on computers that are not part of the City's network, except for third party service providers as approved by the City.
4. Customer account information shall not be stored on external electronic media, except under such conditions as may be approved by the Finance Director.

D. Each employee with access to customer account information will comply with the following policies:

1. File cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with confidential information will be locked or kept in a locked room when not in use.
2. Storage rooms containing documents with confidential 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 confidential information when not in use.
4. When documents containing confidential information are discarded they will be placed inside a locked shred bin or immediately shredded. Municipal records, however, may only be destroyed in accordance with the city's records retention policy.
5. Confidential information shall not be transmitted by e-mail, except as approved by the Finance Director, and using such protections as may be directed by the Finance Director.
6. Confidential information subject to the above provisions includes taxpayer identification numbers, social security numbers, bank account information and any other information which may hereafter be designated as a private record under the laws of the State of Tennessee.

E. If a City employee detects a Red Flag, the employee shall notify the Finance Director. The Finance Director shall undertake such additional measures as may be necessary to determine whether the Red Flag indicates the possibility of identity theft. The Finance Director may take one or more of the following steps to prevent identity theft:

1. Monitoring a customer account for evidence of identity theft;
2. Closing an existing customer account;
3. Not attempting to collect on a customer account;
4. Notifying the customer or other person who may be a victim of identity theft;
5. Notifying law enforcement; or
6. Determining that no response is warranted under the particular circumstances.

F. If the City discovers that any person has become a victim of identity theft, the City shall notify the victim and local law enforcement, and shall cooperate with law enforcement investigations.

SECTION IV. PROGRAM UPDATES

The City shall review the Program at least annually and shall update the Program as needed to reflect changes in identity theft risks. In updating the Program, the City shall consider the following:

A. The City's experiences with identity theft.
B. Changes in methods of identity theft.
C. Changes in methods to detect, prevent, and mitigate identity theft.
D. Changes in the City's types of customer accounts.
E. Changes in business arrangements, such as those involving third party service providers and billing agreements with other utilities.

SECTION V. PROGRAM ADMINISTRATION

A. The Program shall be approved by the Board of Mayor and Aldermen. The Finance Director shall oversee the administration of the Program and may assign specific responsibility for the implementation and administration of various elements of the Program to other City employees.

B. Staff training shall be conducted annually for all employees who may have access to or come into contact with customer accounts or personally identifiable information of the City's utility customers. The Finance Director is responsible for ensuring that such training takes place and that it appropriately familiarizes employees with this Program. Whenever changes to the Program are made, training updates will be carried out as needed.

C. The Finance Director shall prepare and present a written report to the Board of Mayor and Aldermen at least annually on the City's compliance with the Red Flag Rules. The report to the Board of Mayor and Aldermen shall include a discussion of the following:

1. The effectiveness of the Program in addressing the risk of identity theft.
2. Third party service provider arrangements.
3. Significant incidents of identity theft and management's response.
4. Recommendations for changes to the Program.

D. The City has business relationships with third party service providers for billing services, backflow prevention, maintaining a secure website, collection of delinquent accounts and other services. Under these business relationships, the third-party service providers have access to customer identifying information covered under this Program. 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. 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 as meeting these

requirements. The Finance Director shall ensure that a third-party service providers' work for the City is consistent with this Program by:

(1) Ensuring that contracts with the third-party service providers incorporate these requirements; or

(2) Determining that the third-party service providers have reasonable alternative safeguards that provide the same or a greater level of protection for customer identifying information as provided by the City.

EFFECTIVE DATE:
June 15, 2020