TITLE III: ADMINISTRATION

Chapter

CHAPTER 30: TOWN ORGANIZATION

Section

Auxiliary Police

AUXILIARY POLICE

§ 30.01 AUXILIARY POLICE DIVISION ESTABLISHED.

There is hereby established within the town's Police Department, as a division thereof, an Auxiliary Police Division. The Auxiliary Police Division shall be a volunteer organization whose members shall serve without compensation, composed of as many members as may from time to time be determined by the Chief of Police and approved by the Town Administrator.
(Ord. 107, passed 4-5-2004)

CHAPTER 31: TOWN POLICIES

Section

General Provisions

Identity Theft Program

GENERAL PROVISIONS

§ 31.01 CONCEALED WEAPONS PROHIBITED ON TOWN PROPERTY.

(A) *Posting of signs required.* The town's Police Department is hereby authorized and instructed to post conspicuous signage at appropriate locations on or within each park and each building or portion of a building owned, leased as lessee, operated, occupied, managed, or controlled by the town, as well as the appurtenant premises to such buildings, indicating that carrying a concealed handgun is prohibited therein.

(B) *Location of signs.* Signs on buildings shall be visibly posted on the exterior of each entrance by which the general public can access the building. The town's Police Department shall exercise discretion

in determining the number and appropriate location of signs to be placed on or within appurtenant premises and parks.
(Ord. 82-A, passed 2-5-1996) Penalty, see § 10.99

§ 31.02 DISPOSAL OF PERSONAL PROPERTY VALUED AT LESS THAN $5,000.

(A) The Town Administrator is hereby authorized to dispose of any surplus personal property owned by the town whenever he or she determines, in his or her discretion, that:

(1) The item or group of items has a fair market value of less than $5,000;

(2) The property is no longer necessary for the conduct of public business; and

(3) Sound property management principles and financial considerations indicate that the interests of the town would best be served by disposing of the property.

(B) The Town Administrator may dispose of any such surplus personal property by any means which he or she judges reasonably calculated to yield the highest attainable sale price in money or other consideration, including, but not limited to, the methods of sale provided in G.S. Ch. 160A, Art. 12. Such sale may be public or private, and with or without notice and minimum waiting period.

(C) The surplus property shall be sold to the party who tenders the highest offer, or exchanged for any property or services useful to the town if greater value may be obtained in that manner, and the Town Administrator is hereby authorized to execute and deliver any applicable title documents. If no offers are received within a reasonable time, the Town Administrator may retain the property, obtain any reasonably available salvage value, or cause it to be disposed of as waste material. No surplus property may be donated to any individual or organization except by resolution of the Town Council.

(D) The Town Administrator shall keep a record of all property sold under authority of this section and that record shall generally describe the property sold or exchanged, to whom it was sold, or with whom exchanged, and the amount of money or other consideration received for each sale or exchange.

(E) This section is enacted pursuant to the provisions of G.S. § 160A-266(c).
(Ord. 91, passed 6-15-1998)

IDENTITY THEFT PROGRAM

§ 31.15 PROGRAM ADOPTION.

The Town Utility Department ("Utility") developed this Identity Theft Prevention Program ("Program") pursuant to the Federal Trade Commission's Red Flags Rule ("Rule"), which implements

§ 114 of the Fair and Accurate Credit Transactions Act of 2003 (16 C.F.R. § 681.2). This Program was developed with oversight and approval of the Town Council. After consideration of the size and complexity of the Utility's operations and account systems, and the nature and scope of the Utility's activities, the Town Council determined that this Program was appropriate for Town Utilities, and therefore approved this Program on October 6, 2008.
(Ord. 131, passed 10-6-2008)

§ 31.16 FULFILLING REQUIREMENTS OF THE RED FLAGS RULE.

(A) Under the Red Flag Rule, every financial institution and creditor is required to establish an "Identity Theft Prevention Program" tailored to its size, complexity, and the nature of its operation.

(B) Each program must contain reasonable policies and procedures to:

(1) Identify relevant red flags for new and existing covered accounts and incorporate those red flags into the Program;

(2) Detect red flags that have been incorporated into the Program;

(3) Respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and

(4) Ensure the Program is updated periodically, to reflect changes in risks to customers or to the safety and soundness of the creditor from identity theft.
(Ord. 131, passed 10-6-2008)

§ 31.17 RED FLAGS RULE DEFINITIONS USED IN THIS PROGRAM.

(A) The Red Flags Rule defines ***IDENTITY THEFT*** as fraud committed using the identifying information of another person and a ***RED FLAG*** as a pattern, practice, or specific activity that indicates the possible existence of identity theft.

(B) According to the Rule, a municipal utility is a creditor subject to the Rule requirements. The Rule defines ***CREDITORS*** to include finance companies, automobile dealers, mortgage brokers, utility companies, and telecommunications companies. Where nonprofit and government entities defer payment for goods or services, they, too, are to be considered creditors.

(C) All the utility's accounts that are individual utility service accounts held by customers of the utility whether residential, commercial, or industrial are covered by the Rule. Under the Rule, a ***COVERED ACCOUNT*** is:

(1) Any account the Utility offers or maintains primarily for personal, family, or household purposes, that involves multiple payments or transactions; and

(2) Any other account the Utility offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the Utility from identity theft.

(D) ***IDENTIFYING INFORMATION*** is defined under the Rule as any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including: name, address, telephone number, Social Security number, date of birth, government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, unique electronic identification number, computer's internet protocol address, or routing code.
(Ord. 131, passed 10-6-2008)

§ 31.18 IDENTIFICATION OF RED FLAGS.

(A) In order to identify relevant red flags, the Utility considers the types of accounts that it offers and maintains, the methods it provides to open its accounts, the methods it provides to access its accounts, and its previous experiences with identity theft.

(B) The Utility identifies the following red flags, in each of the listed categories.

(1) *Notifications and warnings from credit reporting agencies red flags.*

(a) Report of fraud accompanying a credit report;

(b) Notice or report from a credit agency of a credit freeze on a customer or applicant;

(c) Notice or report from a credit agency of an active duty alert for an applicant; and

(d) Indication from a credit report of activity that is inconsistent with a customer's usual pattern or activity.

(2) *Suspicious documents red flags.*

(a) Identification document or card that appears to be forged, altered, or inauthentic;

(b) Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;

(c) Other document with information that is not consistent with existing customer information (such as if a person's signature on a check appears forged); and

(d) Application for service that appears to have been altered or forged.

(3) *Suspicious personal identifying information red flags.*

(a) Identifying information presented that is inconsistent with other information the customer provides (example: inconsistent birth dates);

(b) Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a credit report);

(c) Identifying information presented that is the same as information shown on other applications that were found to be fraudulent; and

(d) Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address):

1. Social Security number presented that is the same as one given by another customer;

2. An address or phone number presented that is the same as that of another person;

3. A person fails to provide complete personal identifying information on an application when reminded to do so (however, by law Social Security numbers must not be required); and

4. A person's identifying information is not consistent with the information that is on file for the customer.

(4) *Suspicious account activity or unusual use of account red flags.*

(a) Change of address for an account followed by a request to change the account holder's name;

(b) Payments stop on an otherwise consistently up-to-date account;

(c) Account used in a way that is not consistent with prior use (example: very high activity);

(d) Mail sent to the account holder is repeatedly returned as undeliverable;

(e) Notice to the Utility that a customer is not receiving mail sent by the Utility;

(f) Notice to the Utility that an account has unauthorized activity;

(g) Breach in the Utility's computer system security; and

(h) Unauthorized access to or use of customer account information.

(5) *Alerts from others red flag*. Notice to the Utility from a customer, identity theft victim, law enforcement, or other person that it has opened or is maintaining a fraudulent account for a person engaged in identity theft.
(Ord. 131, passed 10-6-2008)

§ 31.19 DETECTING RED FLAGS.

(A) *New accounts*. In order to detect any of the red flags identified above associated with the opening of a new account, Utility personnel will take the following steps to obtain and verify the identity of the person opening the account:

(1) Require certain identifying information such as name, date of birth, residential or business address, principal place of business for an entity, driver's license, or other identification;

(2) Verify the customer's identity (for instance, review a driver's license or other identification card);

(3) Review documentation showing the existence of a business entity; and

(4) Independently contact the customer.

(B) *Existing accounts*. In order to detect any of the red flags identified above for an existing account, Utility personnel will take the following steps to monitor transactions with an account:

(1) Verify the identification of customers if they request information (in person, via telephone, via facsimile, or via email);

(2) Verify the validity of requests to change billing addresses; and

(3) Verify changes in banking information given for billing and payment purposes.
(Ord. 131, passed 10-6-2008)

§ 31.20 PREVENTING AND MITIGATING IDENTITY THEFT.

In the event Utility personnel detect any identified red flags, such personnel shall take one or more of the following steps, depending on the degree of risk posed by the red flag.

(A) *Prevent and mitigate*.

(1) Continue to monitor an account for evidence of identity theft;

(2) Contact the customer;

(3) Change any passwords or other security devices that permit access to accounts;

(4) Not open a new account;

(5) Close an existing account;

(6) Reopen an account with a new number;

(7) Notify the Program Administrator for determination of the appropriate step(s) to take;

(8) Notify law enforcement; and/or

(9) Determine that no response is warranted under the particular circumstances.

(B) *Protect customer identifying information*. In order to further prevent the likelihood of identity theft occurring with respect to Utility accounts, the Utility will take the following steps with respect to its internal operating procedures to protect customer identifying information:

(1) Ensure that its website is secure or provide clear notice that the website is not secure;

(2) Ensure complete and secure destruction of paper documents and computer files containing customer information;

(3) Ensure that office computers are password protected and that computer screens lock after a set period of time;

(4) Keep offices clear of papers containing customer information;

(5) Request only the last four digits of Social Security numbers (if any);

(6) Ensure computer virus protection is up to date; and

(7) Require and keep only the kinds of customer information that are necessary for utility purposes.
(Ord. 131, passed 10-6-2008)

§ 31.21 PROGRAM UPDATES.

This Program will be periodically reviewed and updated to reflect changes in risks to customers and the soundness of the Utility from identity theft. At least every two years, the Program Administrator will consider the Utility's experiences with identity theft situation, changes in identity theft methods, changes in identity theft detection and prevention methods, changes in types of accounts the Utility maintains and changes in the Utility's business arrangements with other entities. After considering these factors, the Program Administrator will determine whether changes to the Program, including the listing of red flags,

are warranted. If warranted, the Program Administrator will update the Program or present the County Board of Commissioners with his or her recommended changes and the County Board of Commissioners will make a determination of whether to accept, modify, or reject those changes to the Program.
(Ord. 131, passed 10-6-2008)

§ 31.22 OVERSIGHT.

Responsibility for developing, implementing, and updating this Program lies with an Identity Theft Committee for the Utility. The Committee is headed by a Program Administrator who may be the head of the Utility or his or her appointee. Two or more other individuals appointed by the head of the Utility or the Program Administrator comprise the remainder of the Committee membership. The Program Administrator will be responsible for the Program administration, for ensuring appropriate training of Utility staff on the Program, for reviewing any staff reports regarding the detection of red flags and the steps for preventing and mitigating identity theft, determining which steps of prevention and mitigation should be taken in particular circumstances, and considering periodic changes to the Program.
(Ord. 131, passed 10-6-2008)

§ 31.23 STAFF TRAINING AND REPORTS.

Utility staff responsible for implementing the Program shall be trained either by or under the direction of the Program Administrator in the detection of red flags, and the responsive steps to be taken when a red flag is detected. (The Utility may include in its Program how often training is to occur. The Program may also require staff to provide reports to the Program Administrator on incidents of identity theft, the Utility's compliance with the Program and the effectiveness of the Program.)
(Ord. 131, passed 10-6-2008)

§ 31.24 SERVICE PROVIDER ARRANGEMENTS.

In the event the Utility engages a service provider to perform an activity in connection with one or more accounts, the Utility will take the following steps to ensure the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft:

(A) Require, by contract, that service providers have such policies and procedures in place; and

(B) Require, by contract, that service providers review the Utility's Program and report any red flags to the Program Administrator.
(Ord. 131, passed 10-6-2008)

§ 31.25 SPECIFIC PROGRAM ELEMENTS AND CONFIDENTIALITY.

For the effectiveness of identity theft prevention programs, the Red Flag Rule envisions a degree of confidentiality regarding the Utility's specific practices elating to identity theft detection, prevention, and mitigation. Therefore, under this Program, knowledge of such specific practices is to be limited to the Identity Theft Committee and those employees who need to know them for purposes of preventing identity theft. Because this Program is to be adopted by a public body and thus publicly available, it would be counterproductive to list these specific practices here. Therefore, only the Program's general red flag detection, implementation, and prevention practices are listed in this document.
(Ord. 131, passed 10-6-2008)

CHAPTER 32: STATE OF EMERGENCY

Section

§ 32.01 REASONS FOR DECLARING A STATE OF EMERGENCY.

A state of emergency shall be deemed to exist whenever, during times of great public crisis, disaster, rioting, catastrophe, or similar public emergency, for any reason, municipal public safety authorities are unable to maintain public order or afford adequate protection for lives, safety, or property.
(Ord. 79, passed 12-7-1994)

§ 32.02 NOTICE AND CURFEW.

In the event of an existing or threatened state of emergency endangering the lives, safety, health, and welfare of the people within the town, or threatening damage to or destruction of property, the Mayor of the town is hereby authorized and empowered to issue a public proclamation declaring to all persons the existence of such a state of emergency, and, in order more effectively to protect the lives and property of the people within the town, to define and impose a curfew and to place in effect any or all of the restrictions hereinafter authorized.
(Ord. 79, passed 12-7-1994)

§ 32.03 MAYOR TO DETERMINE RESTRICTIONS ON THE PUBLIC.

The Mayor is hereby authorized and empowered to limit by the proclamation the application of all or any part of such restrictions to any area specifically designated or described within the corporate limits of the town and to specific hours of the day or night; and to exempt from all or any part of such restrictions law enforcement officers, firefighters, and other public employees, doctors, nurses, employees of hospitals, and other medical facilities; on-duty military personnel, whether state or federal; on-duty employees of public utilities, public transportation companies, and newspaper, magazine, radio

broadcasting, television broadcasting organizations, and other media; and such other classes of persons as may be essential to the preservation of public order and immediately necessary to serve the safety, health, and welfare needs of the people within the town.
(Ord. 79, passed 12-7-1994)

§ 32.04 ENDING A STATE OF EMERGENCY.

The Mayor shall proclaim the end of such state of emergency or all or any part of the restrictions imposed as soon as circumstances warrant or when directed to do so by the Town Council.
(Ord. 79, passed 12-7-1994)

§ 32.05 POSSIBLE RESTRICTIONS THAT MAY BE IMPOSED.

During the existence of a proclaimed state of emergency, the Mayor may impose by proclamation any or all of the following restrictions:

(A) Prohibit, restrict, or regulate the possession, off one's own premises, of explosives, firearms, ammunition, or dangerous weapons of any kind, and prohibit the purchase, sale, transfer, or other disposition thereof;

(B) Prohibit, restrict, or regulate the transportation, the buying or selling of beer, wine, or intoxicating beverages of any kind, and their possession or consumption off one's own premises;

(C) Prohibit, restrict, or regulate any movements of people in public places or any demonstration, parade, march, vigil, or participation therein from taking place on any of the public ways or upon any public property;

(D) Prohibit, restrict, or regulate the sale of gasoline, kerosene, naphtha, or any other explosive or inflammable fluids or substances;

(E) Prohibit, restrict, or regulate travel upon any public street, alley, or roadway or upon any other public property, except by those in search of medical assistance, food, or other commodity or service necessary to sustain the well-being of themselves or their families or some member thereof;

(F) Prohibit, restrict, or regulate the participation in or carrying on of any business activity, and prohibit or regulate the keeping open of places of business/places of entertainment, and any other places of public assembly; and

(G) Prohibit, restrict, or regulate such other activities or conditions, the control of which is reasonably necessary to maintain order and protect lives or property during the existence of the state of emergency.
(Ord. 79, passed 12-7-1994)

§ 32.06 MODIFICATION OF INITIAL PROCLAMATION.

Any proclamation may be extended, altered, or repealed in any particular during the continued or threatened existence of a state of emergency by the issuance of a subsequent proclamation.
(Ord. 79, passed 12-7-1994)

§ 32.07 VIOLATION OF PROCLAMATION PROHIBITED.

During the existence of a proclaimed state of emergency, it shall be unlawful for any person to violate any provision of any restriction imposed by any proclamation authorized by this subchapter, and any such person shall be punished as provided by applicable law as of the time of such violation.
(Ord. 79, passed 12-7-1994) Penalty, see § 10.99