account is a covered account; and

WHEREAS, the Federal Trade Commission regulations require each creditor to adopt an Identity Theft Prevention Program which will use red flags to detect, prevent and mitigate identity theft related information used in covered accounts; and

WHEREAS, the City provides water and sewer services for which payment is made after the product is consumed or the service has otherwise been provided which by virtue of being utility accounts are covered accounts; and

WHERAS, the City Attorney has reviewed the policies and procedures of the Tontitown Water and Sewer Department and believes the proposed additions herein to the Municipal Code fulfills, complies and implements the Red Flags Rule and other requirements outlined by the Federal Trade Commission; and

WHEREAS, the City Council hereby finds that it is in the public interest to approve and adopt the language herein, as part of the City Code, in compliance with FTC requirements.

NOW, THEREFORE, BE IT ORDAINED BY THE CITY COUNCIL OF THE CITY OF TONTITOWN, ARKANSAS, FOR THE PURPOSE OF ADOPTING THE FOLLOWING IDENTITY THEFT PREVENTION PROGRAM THAT:

SECTION 1: The foregoing recitals are hereby found to be true and correct and are hereby adopted by the City Council and made a part hereof for all purposes.

SECTION 2: The Code of Ordinances for the City of Tontitown, Arkansas, is hereby amended by adding Title V, Chapter 54, to read as follows:

"CHAPTER 54"

Identity Theft Prevention Program

54.01 Short Title: This Chapter shall be known as the 'Tontitown Identity Theft Prevention Program.'

54.02 Purpose: The purpose of this Chapter is to comply with 16 CFR § 681.2 in order to detect, prevent and mitigate identity theft by identifying an detecting identity theft red flags and by responding to such red flags in a manner that will prevent identity theft.

54.03 Definitions: For purposes of this Chapter, the following definitions apply:

(a) 'City' means the City of Tontitown.

(b) 'Covered account' means (I) An account that a financial institution or

creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account; and (ii) Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

(c) 'Credit' means the right granted by a creditor to a debtor to defer payment of a debt or to incur debts and defer its payment or to purchase property or services and defer payment therefore.

(d) 'Creditor' means any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit and includes utility companies and telecommunications companies.

(e) 'Customer' means a person that has a covered account with a creditor.

(f) 'Identity theft' means a fraud committed or attempted using identifying information of another person without authority.

(g) 'Person' means a natural person, a corporation, government or governmental subdivision or agency, trust, estate, partnership, cooperative, or association.

(h) 'Personal Identifying Information' includes but is not limited to a person's credit card account information, debit card information, bank account information and drivers' license information and for a natural person includes their social security number, mother's birth name, and date of birth.

(i) 'Red flag' means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

(j) 'Service provider' means a person that provides a service directly to the city.

54.04 Findings. The Federal Trade Commission ("FTC") requires every utility, including public water and sewer systems, such as the Tontitown Water and Sewer Department,

to implement an Identity Theft Prevention Program ("ITPP"). The FTC requirements and regulations are necessary because of § 114 of the Fair and Accurate Credit Transactions Act ("FACTA"). The TRC has set forth the ITPP requirement in 16 C.F.R. § 681.2. Identity theft is defined as a fraud committed or attempted using identifying information of another person without authority. The City of Tontitown adopts the program set forth in this Chapter to comply with FTC rules and regulations. In drafting its ITPP, the City has considered: (1) the methods it provides to open its accounts; (2) the methods it provides to access its accounts; and (3) its previous experiences with identity theft. Based on these considerations, the City Council hereby determines that the City Water & Sewer Department is a low to moderate risk entity, and as a result develops and implements the streamlined ITPP set forth hereto. Further, the City determines that the only covered accounts offered by the City are those under its water and sewer utilities.

54.05 Red Flats: The FTC regulations identify numerous red flags that must be considered in adopting an ITPP. The FTC has defined a red flag as a pattern, practice, or specific activity that indicates the possible existence of identity theft. The City identifies the following red flags from the examples provided in the regulations of the FTC:

(a) Notifications from Consumer Reporting Agencies: The City does not request, receive, obtain or maintain information about its utility customers from any Consumer Reporting Agency.

(b) Suspicious documents - Possible red flags include:

i) presentation of documents appearing to be altered or forged;

ii) presentation of photographs or physical descriptions that are not consistent with the appearance of the applicant or customer;

iii) presentation of other documentation that is not consistent with the information provided when the account was opened or existing customer information;

iv) presentation of information that is not consistent with the account application; or

v) presentation of an application that appears to have been altered, forged, destroyed, or reassembled.

(c) Suspicious personal identifying information - Possible red flags include:

i) personal identifying information is being provided by the customer that is not consistent with other personal identifying information provided by the customer or is not consistent with the customer's account application;

ii) personal identifying information associated with known fraudulent activity;

iii) the social security number (if required or obtained) is the same as that submitted by another customer;

iv) the telephone number or address is the same as that submitted by another customer;

v) the applicant's failure to provide all personal identifying information requested on the application; or

vi) the applicant or customer's inability to provide authenticating information beyond that which generally would be available to a consumer.

(d) Unusual use or suspicious activity related to an account - Possible red flags include:

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

ii) a change of address for an account followed by a request to add new or additional authorized users or representatives;

iii) an account is not being used in a way that is consistent with prior use (such as late or no payments when the account has been timely in the past);

iv) a new account is used in a manner commonly associated with known patterns of fraudulent activity (such as customer fails to make the first payment or makes the first payment but not subsequent payments);

v) mail sent to the account holder is repeatedly returned as undeliverable;

vi) the City receives notice that a customer is not receiving his paper statements; or

vii) the City receives notice of unauthorized activity on the account.

(e) Notice regarding possible identity theft - Possible red flags include:

i) notice from a customer, an identity theft victim, law enforcement personnel or other reliable sources regarding possible identity theft or phishing related to utility accounts.

54.06 Red Proof of Identity: Any person or entity opening a utility account shall provide a complete application and provide satisfactory evidence of their identity and/or address. Said proof may include but not be limited to: a valid driver's license; passport; state, federal, employer, or school issued identification card; or military identification card. The required application must be completed in its entirety and must be signed in order to establish a utility account.

54.07 Red Confidentiality of Applications and Account Information: All personal information, personal identifying information, account applications and account information collected and maintained by the City shall be a confidential record of the City and shall not be subject to disclosure unless otherwise required by State and Federal Law. Additionally, any employee with access to utility customers' personal information, account applications or account information shall be required to keep such information in confidence and protect the privacy of Customers, and may be required to execute and abide by a written Confidentiality and Non-Disclosure Policy.

54.08 Red Access to utility account information: Access to utility account information shall be limited to employees that provide customer service and technical support to the City's utilities. Any computer that has access to utility customer account or personal identifying information shall be password protected and all computer screens shall lock after no more than fifteen (15) minutes of inactivity. All paper and non-electronic based utility account or customer personal identifying information shall be stored and maintained in a locked room or cabinet and access shall only be granted by the Compliance Officer or his/her designee, or in the alternative shall be scanned for secure, password protected, digital storage, and then shredded.

54.09 Red Credit Card Transactions: In the event credit cards are added as a payment option for utility accounts, all internet or telephone credit card payments shall only be processed through a third-party service provider which certifies that it has an identity theft prevention program operating and in place. Credit card payments accepted in person shall require a reasonable connection between the person or entity billed for the utility services and the credit card owner.

54.10 Red Suspicious Transactions: Suspicious transactions include but are not limited to the presentation of incomplete applications; unsigned applications; payment by

someone other than the person named on the utility account; presentation of inconsistent signatures, addresses or identification. Suspicious transactions shall not be processed and shall be immediately referred to the Compliance Officer.

54.11 Notification of Law Enforcement: The Executive Director of the Water and Sewer Commission shall use his/her discretion on whether to report suspicious transactions to the police department or other appropriate law enforcement.

54.12 Third-Party Service Providers: All transactions process through a third-party service provider shall be permitted only if the service provider certifies that it has complied with the FTC regulations and has in place a consumer identity theft prevention program.

54.13 Compliance Officer and Training: The "Compliance Officer" for this ITPP and Chapter shall be the Executive Director of the Water and Sewer Commission or his/her designee. The Compliance Officer shall conduct training of all city utility employees that transact business with customers of the City's utilities. The Compliance Officer shall periodically review this program and recommend any necessary updates to the City Council.

54.14 Annual Report: An annual report, as required by the FTC regulations, shall be provided by the Water & Sewer Department Superintendent/Director to the Mayor and City Council. The contents of the annual repot shall address and/or evaluate at least the following:

(a) the effectiveness of the policies and procedures of the City in addressing the risk of identity theft in connection with the opening of utility accounts and with respect to access to existing utility accounts; and

(b) software, credit-card processing, and service provider arrangements; and

(c) any incidents involving identity theft, or suspected identity theft, with utility accounts and the City's remedial response; and

(d) any changes, or proposed changes, in methods to identify identity theft and/or to prevent identity theft; and

(e) any recommendations for changes or modifications to the City's ITPP.

SECTION 3: The various provisions and parts of this Ordinance are hereby declared to be severable, and, if any section or part of a section, or any provision or part of a

provision herein, is declared to be unconstitutional, inappropriate, or invalid by any court of competent jurisdiction, such holding shall not invalidate or affect the remainder of this Ordinance and to that extent the provisions hereto are declared to be severable.

SECTION 4: All ordinances, resolutions or other acts of the City in conflict with the terms hereof are repealed or amended to the extent of any such conflict.

PASSED AND APPROVED THIS 2nd DAY OF December, 2008.

Mayor

Debra A. Conten
Recorder-Treasurer