

ORDINANCE NO. 2009-11

TOWN OF HIGHFILL, BENTON COUNTY, ARKANSAS

AN ORDINANCE TO ESTABLISH AN “IDENTITY THEFT PREVENTION PROGRAM” IN COMPLIANCE WITH FEDERAL REGULATIONS; TO COMPLY WITH FEDERAL REGULATIONS RELATING TO ADDRESS DISCREPANCIES; TO COMPLY WITH FEDERAL REGULATIONS RELATING TO RED FLAGS AND IDENTITY THEFT; TO PROVIDE FOR SEVERABILITY; TO PROVIDE FOR AN ADOPTION DATE; TO PROVIDE AN EFFECTIVE DATE; AND FOR OTHER PURPOSES ALLOWED BY LAW.

WHEREAS, pursuant to federal law the Federal Trade Commission adopted Identity Theft Rules requiring the creation of certain policies relating to the use of consumer reports, address discrepancy and the detection, prevention and mitigation of identity theft; and

WHEREAS, in implementing § 114 of the FAIR AND ACCURATE CREDIT TRANSACTIONS ACT OF 2003, the Federal Trade Commission has adopted regulations, as set forth in 16 CFR § 681.2 pertaining to Identity Theft Protection, which require creditors, as defined by 15 U.S.C. § 1681a(r)(5), to adopt red flag policies to prevent and mitigate identity theft with respect to covered accounts; and

WHEREAS, 15 U.S.C. § 1681a(r)(5) cites 15 U.S.C. § 1691a, which defines a creditor as a person that extends, renews or continues credit, and defines ‘credit’ in part as the right to purchase property or services and defer payment therefore; and

WHEREAS, the Federal Trade Commission regulations specifically include municipal utility companies in the definition of creditor; and

WHEREAS, the Town of Highfill (the “Town”) is a ‘creditor’ with respect to 16 CFR § 681.2 by virtue of providing utility services, or by otherwise accepting payment for municipal services in arrears; and

WHEREAS, the Federal Trade Commission regulations define ‘covered account’ in part as an account that a creditor provides for personal, family or household purposes that is designed to allow multiple payments or transactions and specifies that a utility 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 to information used in covered accounts; and

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

WHEREAS, the duly elected governing authority of the Town of Highfill is the Mayor and Council thereof, and the Council hereby finds that it is in the best interest of the Town and its citizens to approve and adopt the language set forth herein in compliance with the Federal Trade Commission requirements.

NOW THEREFORE, BE IT ENACTED, by the Town Council of the Town of Highfill, as follows:

Identity Theft Prevention Program

Section 1. Short Title. This shall be known, and may be cited, as the “Highfill Identity Theft Prevention Program.”

Section 2. Purpose. The purpose hereof is to comply with 16 CFR § 681.2 in order to detect, prevent and mitigate identity theft by identifying and detecting identity theft red flags and by responding to such red flags in a manner that will prevent identity theft.

Section 3. Definitions. For purposes hereof, the following definitions apply¹:

- (a) ‘*City*’ means the Town of Highfill, Arkansas.
- (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 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

¹ Other than “city” and “personal identifying information”, definitions provided in this section are based on the definitions provided in 16 CFR § 681.2.

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*’ means 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.

Section 4. Determinations. The Federal Trade Commission (“FTC”) requires every utility, including public water and sewer systems, such as the Highfill Water and Sewer Department, to implement an Identity Theft Protection Program (“ITPP”). Identity theft is defined as a fraud committed or attempted using identifying information of another person without authority. The City adopts the program set forth herein to comply with the FTC rules and regulations, and in connection with preparing and implementing such a program 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 Highfill Water and Sewer Departments is a low to moderate risk entity, and as a result develops and implements the streamlined ITPP set forth herein. Further, the City determines that the only covered accounts offered by the City are those under its water and sewer utilities.

Section 5. Establishing Account; 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;
- (b) Valid passport;
- (c) State, federal, employer, or school-issued identification card; or
- (d) Military identification card

The required application must be completed in its entirety and must be signed in order to establish a utility account.

Section 6. 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 or 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.

Section 7. 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 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.

Section 8. 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 service and the credit card owner.

Section 9. Red Flags. 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) Notification 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:
 - 1. Presentation of documents appearing to be altered or forged;
 - 2. Presentation of photographs or physical descriptions that are not consistent with the appearance of the applicant or customer;

3. Presentation of other documentation that is not consistent with the information provided when the account was opened or existing customer information;
 4. Presentation of information that is not consistent with the account application; or
 5. Presentation of an application that appears to have been altered, forged, destroyed, or reassembled.
- (c) Suspicious personal identifying information – Possible red flags include:
1. 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;
 2. Personal identifying information is associated with known fraudulent activity;
 3. The social security number (if required or obtained) is the same as that submitted by another customer;
 4. The telephone number or address is the same as that submitted by another customer;
 5. The applicant's failure to provide all personal identifying information requested on the application; or
 6. The applicant or customer's inability to provide authenticating information beyond that which generally would be available to a consumer.
- (d) Unusual use of or suspicious activity related to an account – Possible red flags include:
1. A change of address for an account followed by a request to change the account holder's name;
 2. A change of address for an account followed by a request to add new or additional authorized users or representatives;

3. 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);
 4. 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 no subsequent payments);
 5. Mail sent to the account holder is repeatedly returned as undeliverable;
 6. The City receives notice that a customer is not receiving his paper statements; or
 7. The City receives notices of unauthorized activity on the account.
- (e) Notice regarding possible identity theft – Possible red flags include:
1. 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.

Section 10. Suspicious Transactions. Suspicious transactions include but are not limited to:

- (a) Presentation of incomplete applications;
- (b) Unsigned applications;
- (c) Payment by someone other than the person named on the utility account;
- (d) Presentation of inconsistent signatures, addresses or identification. Suspicious transactions shall not be processed and shall be immediately referred to the Compliance Officer.

Section 11. Notification of Law Enforcement. The Water Superintendent/Director shall use his/her discretion on whether to report suspicious transactions to the police department or other appropriate law enforcement.

Section 12. Third-Party Service Providers. All transactions processed 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.

Section 13. Compliance Officer and Training. The “Compliance Officer” for this ITPP shall be the Water Superintendent/Director or his/her designee, who shall be responsible for oversight of the program and for program implementation. 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 exercise his or her discretion in determining the amount and substance of training necessary. Further, the Compliance Officer shall periodically review this program and recommend any necessary updates to the City Council.

Section 14. Annual Report. An annual report, as required by FTC regulations, shall be provided by the Compliance Officer to the Mayor and City Council. The contents of the annual report 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;
- (b) Software, credit-card processing, and service provider arrangements;
- (c) Any incidents involving identity theft, or suspected identity theft, with utility accounts and the City’s remedial response;
- (d) Any changes, or proposed changes, in methods to identify identity theft and/or prevent identity theft; and
- (e) Any recommendations for changes or modifications to the City’s ITPP.

Section 15. Program Administration. The Mayor is responsible for reviewing the annual report prepared by the Compliance Officer and any other reports prepared by staff regarding compliance with red flag requirements and with recommending material changes to the program, as necessary in the opinion of the Mayor, to address changing identity theft risks and to identify new or discontinued types of covered accounts. Any recommended material changes to the program shall be submitted to the City Council for consideration.

Section 16. Updating the Program. The City Council shall periodically review and, as deemed necessary by the Council, update the Identity Theft Prevention Program along with any relevant red flags in order to reflect changes in risks to customers or to the safety and soundness of the City and its covered accounts from identity theft. In so doing, the City Council shall consider the following factors and exercise its discretion in amending the program:

- (1) The City’s experiences with identity theft;
- (2) Updates in methods of identity theft;

- (3) Updates in customary methods used to detect, prevent, and mitigate identity theft;
- (4) Updates in the types of accounts that the city offers or maintains; and
- (5) Updates in service provider arrangements.

Section 17. Severability Provision. In the event that any section, paragraph, subdivision, clause, phrase, or other provision or portion of this Ordinance shall be adjudged invalid or unconstitutional, the same shall not affect the validity of this Ordinance as a whole, or any part or provision, other than the part so decided to be invalid or unconstitutional, and the remaining provisions of this Ordinance shall be construed as if such invalid, unenforceable or unconstitutional provision or provisions had never been contained herein.

Section 18. Repeal of Conflicting Ordinances and Resolutions. All ordinances and resolutions or parts of ordinances and resolutions in conflict herewith are hereby repealed to the extent of such conflict.

Section 19. Declaration of Emergency. It is hereby found and determined that the Federal Trade Commission, in implementing § 114 of the Fair and Accurate Credit Transactions Act of 2003, is requiring municipal governments that are creditors to adopt an Identity Theft Prevention Program, which will use red flags to detect, prevent and mitigate identity theft related to information used in covered accounts, by May 1, 2009, and the Town of Highfill, being such a creditor, does not currently have such a program in place. Therefore, an emergency is declared to exist, and this act being immediately necessary for the preservation and protection of the public peace, health, safety and welfare of the Town and its citizens, shall become effective on the date of its passage and approval by the Mayor. If the Ordinance is neither approved nor vetoed by the Mayor, it shall become effective on the expiration of the period of time during which the Mayor may veto this Ordinance. If the Ordinance is vetoed by the Mayor and the veto is overridden by the Town Council, it shall become effective on the date the Town Council overrides the veto.

PASSED AND APPROVED this ____ day of _____, 2009.

APPROVED:

Chris Holland, Mayor

ATTEST:

Stacy Digby, Town Recorder

(SEAL)