

**TOWN OF MITCHELL
RESOLUTION TO ADOPT IDENTITY THEFT PREVENTION PROGRAM**

A RESOLUTION TO ADOPT A POLICY TO IMPLEMENT AN IDENTITY THEFT PREVENTION PROGRAM; TO COMPLY WITH FEDERAL REGULATIONS RELATING TO RED FLAGS AND IDENTITY THEFT; TO PROVIDE FOR SEVERABILITY; 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;

WHEREAS, the Federal Trade Commission regulations, adopted as 16 CFR § 681.2 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;

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;

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

WHEREAS, the Town of Mitchell 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;

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;

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

WHEREAS, the Town of Mitchell provides water utility 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;

WHEREAS, customer accounts for solid waste collection for which payment is made after the product is consumed or the service has otherwise been provided are covered accounts by virtue of being for household purposes and allowing for multiple payments or transactions;

WHEREAS, the duly elected governing authority of the Town of Mitchell is the Mayor and council thereof;

THEREFORE BE IT AND IT IS HEREBY RESOLVED AS FOLLOWS:

Section No. 1. Adoption.

The policy containing the Identity Theft Prevention Program attached hereto as Exhibit "A", said exhibit being nine (9) pages, is hereby adopted for use by the Town of Mitchell.

Section No. 2. Severability.

If any article, section, subsection, paragraph, sentence, or part thereof of this resolution shall be held to be invalid or unconstitutional, such invalidity or unconstitutionality shall not affect or impair other parts of this resolution unless it clearly appears that such other parts are wholly and necessarily dependent upon the part or parts held to be invalid or unconstitutional.

Section No. 3. Preamble Incorporated.

The preamble to this resolution is hereby incorporated into the resolution as if set out fully herein.

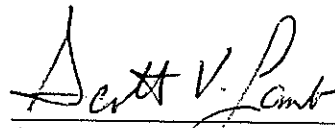
Section No. 4. Repealer.

Any ordinance and/or resolution in conflict with this resolution is hereby repealed.

Section No. 5. Effective Date.

The effective date of this resolution and the attached policy is September 1, 2009.

IN WITNESS WHEREOF, this resolution has been duly adopted by the Mayor and City Council of the Town of Mitchell, Georgia on this 10th day of August, 2009.



Scott V. Lamb Mayor

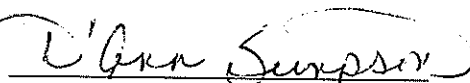
Attested by: 
D'Ann Simpson
City Clerk

Exhibit "A"

Town of Mitchell Identity Theft Prevention Program

Section 1.01. Short Title.

This policy shall be known as the Identity Theft Prevention Program for the Town of Mitchell, Georgia.

Section 1.02. Purpose.

The purpose of this policy 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 1.03. Definitions.

For purposes of this policy, the following definitions apply.

- (a) "City" means the Town of Mitchell.
- (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 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 1.04. Findings.

- (1) The City is a creditor pursuant to 16 CFR § 681.2 due to its provision or maintenance of covered accounts for which payment is made in arrears.
- (2) Covered accounts offered to customers for the provision of city services include water utility accounts and solid waste collection accounts.
- (3) The City’s previous experience with identity theft related to covered accounts is:

Limited. No direct experience.
- (4) The processes of opening a new covered account, restoring an existing covered account and making payments on such accounts have been identified as potential processes in which identity theft could occur.
- (5) The City limits access to personal identifying information to those employees responsible for or otherwise involved in opening or restoring covered accounts or accepting payment for covered accounts. Information provided to such employees is entered directly into the City’s computer system and is not otherwise recorded.
- (6) The City determines that there is a low risk of identity theft occurring in the following ways (if any):
 - a. Use by an applicant of another person’s personal identifying information to establish a new covered account;

- b. Use of a previous customer's personal identifying information by another person in an effort to have service restored in the previous customer's name;
- c. Use of another person's check or other method of payment by a customer to pay such customer's covered account or accounts;
- d. Use by a customer desiring to restore such customer's covered account of another person's check or other method of payment.

Section 1.05. Process of Establishing a Covered Account.

- (1) As a precondition to opening a covered account in the City, each applicant shall provide the City with personal identifying information of the customer to include applicant's full legal name, date of birth, and current mailing address. Applicants shall also provide a valid government issued identification card containing a photograph of the customer or, for customers who are not natural persons, a photograph of the customer's agent opening the account. Such information shall be entered directly into the City's computer system and shall not otherwise be recorded.
- (2) Each account shall be assigned an account number which shall be unique to that account. The City may utilize computer software to randomly generate assigned account numbers and to encrypt account numbers.

Section 1.06. Access to Covered Account Information.

- (1) Access to customer account information shall be password protected and shall be limited to authorized City personnel.
- (2) Such password(s) shall be changed by the City Clerk on a regular basis, shall be at least 8 characters in length and shall contain letters, numbers and symbols.
- (3) Any unauthorized access to or other breach of customer accounts is to be reported immediately to the City Clerk or Mayor and the password changed immediately.
- (4) Personal identifying information included in customer accounts is considered confidential and any request or demand for such information shall be immediately forwarded to the City Clerk and the City Attorney.

Section 1.07. Credit Card Payments.

[Reserved]

Section 1.08. Sources and Types of Red Flags.

All employees responsible for or involved in the process of opening a covered account, restoring a covered account or accepting payment for a covered account shall check for red flags as indicators of possible identity theft and such red flags may include:

- (1) Alerts from consumer reporting agencies, fraud detection agencies or service providers. Examples of alerts include but are not limited to:
 - a. A fraud or active duty alert;
 - b. A notice of credit freeze;
 - c. A notice of address discrepancy.
- (2) Suspicious documents. Examples of suspicious documents include:
 - a. Documents provided for identification that appear to be altered or forged;
 - b. Identification on which the photograph or physical description is inconsistent with the appearance of the applicant or customer;
 - c. Identification on which the information is inconsistent with information provided by the applicant or customer;
 - d. Identification on which the information is inconsistent with readily accessible information that is on file with the creditor, such as a signature on an application or a recent check; or
 - e. An application that appears to have been altered or forged, or appears to have been destroyed and reassembled.
- (3) Suspicious personal identification, such as suspicious address change. Examples of suspicious identifying information include:
 - a. Personal identifying information that is inconsistent with external information sources used by the creditor. For example:
 - i. The address does not match any address in public records; or
 - ii. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.

- b. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer, such as a lack of correlation between the SSN range and date of birth.
 - c. Personal identifying information or a phone number or address, is associated with known fraudulent applications or activities as indicated by internal or third-party sources used by the creditor.
 - d. Other information provided, such as fictitious mailing address, mail drop addresses, jail addresses, invalid phone numbers, pager numbers or answering services, is associated with fraudulent activity.
 - e. The SSN provided is the same as that submitted by other applicants or customers.
 - f. The address or telephone number provided is the same as or similar to the address or telephone number submitted by an unusually large number of applicants or customers.
 - g. The applicant or customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.
 - h. Personal identifying information is not consistent with personal identifying information that is on file with the creditor.
 - i. The applicant or customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.
- (4) Unusual use of or suspicious activity relating to a covered account. Examples of suspicious activity include:
- a. Shortly following the notice of a change of address for an account, City receives a request for modification of the account.
 - b. A new credit account is used in a manner commonly associated with known patterns of fraud. For example:
 - i. The customer fails to make the first payment or makes an initial payment but no subsequent payments.
 - c. An account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:

- i. Nonpayment when there is no history of late or missed payments;
 - ii. A material change in utility usage;
 - d. An account that has been inactive for a long period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).
 - e. Mail sent to the customer is returned repeatedly as undeliverable although utility use continues in connection with the customer's account.
 - f. The City is notified that the customer is not receiving paper account invoices.
 - g. The City is notified of unauthorized charges or transactions in connection with a customer's account.
 - h. The City is notified by a customer, law enforcement or another person that it has opened a fraudulent account for a person engaged in identity theft.
- (5) Notice from customers, law enforcement, victims or other reliable sources regarding possible identity theft or "phishing" relating to covered accounts.

Section 1.09. Prevention and Mitigation of Identity Theft.

- (1) In the event that any City employee responsible for or involved in restoring an existing covered account or accepting payment for a covered account becomes aware of red flags indicating possible identity theft with respect to existing covered accounts, such employee shall use his or her discretion to determine whether such red flag or combination of red flags suggests a threat of identity theft. If, in his or her discretion, such employee determines that identity theft or attempted identity theft is likely or probable, such employee shall immediately report such red flags to the Mayor or Chief of Police. If the Mayor or Chief of Police in his or her discretion determines that further action is necessary, a city employee shall perform one or more of the following responses:
- a. Contact the customer;
 - b. Make the following changes to the account if, after contacting the customer, it is apparent that someone other than the customer has obtained information relating to the customer's covered account:
 - i. change any account numbers, passwords, security codes, or other security devices that permit access to an account; or

- ii. close the account;
 - c. Cease attempts to collect additional charges from the customer and decline to sell the customer's account to a debt collector in the event that the customer's account has been used without authorization and such use has caused additional charges to accrue;
 - d. Notify a debt collector within forty-eight (48) hours of the discovery of likely or probable identity theft relating to a customer account that has been forwarded to such debt collector in the event that a customer's account has been forwarded to such debt collector prior to the discovery of the likelihood or probability of identity theft relating to such account;
 - e. Notify law enforcement, in the event that someone other than the customer has used the customer's account causing additional charges to accrue or has accessed personal identifying information; or
 - f. Take other appropriate action to prevent or mitigate identity theft.
- (2) In the event that any City employee responsible for or involved in opening a new covered account becomes aware of red flags indicating possible identity theft with respect an application for a new account, such employee shall use his or her discretion to determine whether such red flag or combination of red flags suggests a threat of identity theft. If, in his or her discretion, such employee determines that identity theft or attempted identity theft is likely or probable, such employee shall immediately report such red flags to the Mayor or Chief of Police. If the Mayor or Chief of Police in his or her discretion determines that further action is necessary, a city employee shall perform one or more of the following responses:
- a. Request additional identifying information from the applicant;
 - b. Deny the application for the new account;
 - c. Formally notify law enforcement of possible identify theft; or
 - d. Take other appropriate action to prevent or mitigate identity theft.

Section 1.10. Updating the Program.

The city council shall annually 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 thefts;
- (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 1.11. Program Administration.

The City Clerk is responsible for oversight of the program and for program implementation. The City Clerk is responsible for preparing reports regarding compliance with red flag requirements and with recommending material changes to the program, as necessary in the opinion of the City Clerk, 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.

- (1) The City Clerk will report to the Mayor at least annually, on compliance with the red flag requirements. The report will address material matters related to the program and evaluate issues such as:
 - a. The effectiveness of the policies and procedures of City in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts;
 - b. Service provider arrangements;
 - c. Significant incidents involving identity theft and the City's response; and
 - d. Recommendations for material changes to the program.
- (2) The City Clerk is responsible for providing training to all employees responsible for or involved in opening a new covered account, restoring an existing covered account or accepting payment for a covered account with respect to the implementation and requirements of the Identity Theft Prevention Program. The City Clerk shall exercise his or her discretion in determining the amount and substance of training necessary.

Section 1.12. Outside Service Providers.

In the event that the City engages a service provider to perform an activity in connection with one or more covered accounts the City Clerk shall exercise his or her discretion in reviewing such arrangements in order to ensure, to the best of his or her ability, that the service provider's activities are conducted in accordance with policies and procedures, agreed upon by contract, that are designed to detect any red flags that may arise in the performance of the service provider's activities and take appropriate steps to prevent or mitigate identity theft.

[End of Policy]