

# Another Sample

Georgia Municipal Association  
\* Working Draft Sample FACT Act Ordinance \* Note  
September 2008

CITY OF \_\_\_\_\_  
STATE OF GEORGIA

ORDINANCE NO: \_\_\_\_\_

AN ORDINANCE TO AMEND THE CODE OF ORDINANCES, CITY OF \_\_\_\_\_, GEORGIA TO PROVIDE A NEW ARTICLE \_\_\_\_\_, IDENTITY THEFT PREVENTION PROGRAM; TO COMPLY WITH FEDERAL REGULATIONS RELATING TO ADDRESS DISCREPANCIES; TO COMPLY WITH FEDERAL REGULATIONS RELATING TO RED FLAGS AND IDENTITY THEFT; TO PROVIDE FOR CODIFICATION; 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;

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 City of \_\_\_\_\_ is a creditor with respect to 16 CFR § 681.2 by virtue of providing utility services<sup>1</sup> 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;

<sup>1</sup> References to utility accounts only apply to local governments that actually provide utility services. While the regulations state that utility accounts are "covered accounts" and that "creditors" includes utility companies, it is possible that a city could be a creditor with respect to non-utility covered accounts. In this event, the preamble to this ordinance should be amended accordingly.

**Georgia Municipal Association  
Working Draft Sample FACT Act Ordinance  
September 2008**

The purpose of this Article 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 of this Article, the following definitions apply<sup>2</sup>:

- (a) 'City' means the City of \_\_\_\_\_.
- (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, covered 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 covered 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.

---

<sup>2</sup> Other than "city" and "personal identifying information", definitions provided in this section are based on the definitions provided in 16 CFR § 681.2.

containing a photograph of the customer or, for customers who are not natural persons, a photograph of the customer's agent opening the account. If applicable to your city the following could also be included: "Such applicant shall also provide any information necessary for the department providing the service for which the covered account is created to access the applicant's consumer credit report".] 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 and personal identification number (PIN) which shall be unique to that account. The city may utilize computer software to randomly generate assigned PINs and to encrypt account numbers and PINs.

Section \_\_\_\_-6. Access to Covered Account Information.

- (1) Access to customer accounts shall be password protected and shall be limited to authorized city personnel.
- (2) Such password(s) shall be changed by [for example, the director of the department providing the service for which the covered account is created, or by the director of information technology] 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 Manager 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 Manager and the City Attorney.

Section \_\_\_\_-7. Credit Card Payments.

- (1) In the event that credit card payments that are made over the Internet are processed through a third party service provider, such third party service provider shall certify that it has an adequate identity theft prevention program in place that is applicable to such payments.
- (2) All credit card payments made over the telephone or the city's website shall be entered directly into the customer's account information in the computer data base.
- (3) Account statements and receipts for covered accounts shall include only the last four digits of the credit or debit card or the bank account used for payment of the covered account.

Section \_\_\_\_-8. 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:

Georgia Municipal Association  
Working Draft Sample FACT Act Ordinance  
September 2008

- f. The address or telephone number provided is the same as or similar to the account number 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 financial institution or 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 the addition of authorized users on the account.
  - b. A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. 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 purchasing or spending patterns;
  - 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 transactions continue to be conducted in connection with the customer's account.
  - f. The city is notified that the customer is not receiving paper account statements.
  - 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 \_\_\_\_-9. 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

- d. Take other appropriate action to prevent or mitigate identity theft.

Section \_\_\_\_-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 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 \_\_\_\_-11. Program Administration.

*[Senior Level Staff]* is responsible for oversight of the program and for program implementation. The *[City Manager]* is responsible for reviewing 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 *[City Manager]*, to address changing identity theft risks and to identify new or discontinued covered types of covered accounts. Any recommended material changes to the program shall be submitted to the city council for consideration by the council.

- (1) The *[Senior Level Staff]* will report to the *[City Manager]* 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 management's response; and
  - d. Recommendations for material changes to the Program.
- (2) The *[Senior Level Staff]* 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 *[Senior Level Staff]* shall exercise his or her discretion in determining the amount and substance of training necessary.

Section \_\_\_\_-4. Policy.

In the event that the city receives a notice of address discrepancy, the city employee responsible for verifying consumer addresses for the purpose of providing the municipal service or account sought by the consumer shall perform one or more of the following activities, as determined to be appropriate by such employee:

- (1) Compare the information in the consumer report with:
  - a. Information the city obtains and uses to verify a consumer's identity in accordance with the requirements of the Customer Information Program rules implementing 31 U.S.C. § 5318(l);
  - b. Information the city maintains in its own records, such as applications for service, change of address notices, other customer account records or tax records; or
  - c. Information the city obtains from third-party sources that are deemed reliable by the relevant city employee; or
- (2) Verify the information in the consumer report with the consumer.

Section \_\_\_\_-5. Furnishing Consumer's Address to Consumer Reporting Agency.

- (1) In the event that the city reasonably confirms that an address provided by a consumer to the city is accurate, the city is required to provide such address to the consumer reporting agency from which the city received a notice of address discrepancy with respect to such consumer. This information is required to be provided to the consumer reporting agency when:
  - a. The city is able to form a reasonable belief that the consumer report relates to the consumer about whom the city requested the report;
  - b. The city establishes a continuing relation with the consumer; and
  - c. The city regularly and in the ordinary course of business provides information to the consumer reporting agency from which it received the notice of address discrepancy.
- (2) Such information shall be provided to the consumer reporting agency as part of the information regularly provided by the city to such agency for the reporting period in which the city establishes a relationship with the customer.

Section \_\_\_\_-6. Methods of Confirming Consumer Addresses.

The city employee charged with confirming consumer addresses may, in his or her discretion, confirm the accuracy of an address through one or more of the following methods:

- (1) Verifying the address with the consumer;
- (2) Reviewing the city's records to verify the consumer's address;
- (3) Verifying the address through third party sources; or
- (4) Using other reasonable processes.