

## **ARTICLE II. IDENTITY THEFT PREVENTION (RED FLAG) PROGRAM**

### **Section 111-19. Purpose.**

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 111-20. Definitions.**

For purposes of this Article, the following definitions apply:

**City** means the City of Cumming, Georgia.

**Covered account** means

- (1) 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
- (2) 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.

**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.

**Creditor** means:

- (1) Any person who regularly extends, renews, or continues credit; or
- (2) Any person who regularly arranges for the extension, renewal, or continuation of credit; or
- (3) Any assignee of an original creditor who participates in the decision to extend, renew, or continue credit and includes utility companies and telecommunications companies.

**Customer (Consumer)** means a person that has a covered account with a creditor.

**Identity theft** means a fraud committed or attempted using identifying information of another person without authority.

**Notice of address discrepancy** means a notice sent to a user by a consumer reporting agency pursuant to 15 U.S.C. § 1681(c)(h)(1), that informs the user of a substantial difference between the address for the consumer that the user provided to request the consumer report and the address(es) in the agency's file for the consumer

**Person** means a natural person, a corporation, government or governmental subdivision or agency, trust, estate, partnership, cooperative, or association.

**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.

**Red flag** means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

**Service provider** means a person that provides a service directly to the City.

### **Section 111-21. Findings.**

- (a) The City may be a creditor pursuant to 16 CFR § 681.2 due to its provision or maintenance of covered accounts for which payment is made in arrears.
- (b) Covered accounts offered to customers for the provision of City services include water, sewer and garbage services.
- (c) The City has had no negative experience with identity theft related to covered accounts.
- (d) The processes of opening a new covered account, restoring an existing covered account, making payments on such accounts, and closing an account have been identified as potential processes in which identity theft could occur.
- (e) The City limits access to personal identifying information to those employees responsible for or otherwise involved in opening, closing or restoring covered accounts or accepting payment for use of covered accounts. Information provided to such employees is entered directly into the City's computer system and is not otherwise recorded.
- (f) The City determines that there is a low risk of identity theft occurring in the following ways (*if any*):
  - (1) Use by an applicant of another person's personal identifying information to establish a new covered account;
  - (2) 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;
  - (3) Use of another person's credit card, bank account, or other method of payment by a customer to pay such customer's covered account or accounts;
  - (4) Use by a customer desiring to restore such customer's covered account of another person's credit card, bank account, or other method of payment; and
  - (5) Use by another of a customer's personal identifying information to close a customer's account.

### **Section 111-22. Process of Establishing a Covered Account.**

As a precondition to opening a covered account in the City, each applicant shall provide the City with personal identifying information of the customer consisting of either a valid government issued identification card containing a photograph of the customer or, for customers who are not natural persons (corporations, etc.), a valid government issued identification card containing a photograph of the customer's agent opening the account. Upon verification of the customer's identity, the identification card shall be scanned or otherwise entered into the City's computer system and then returned to the customer.

### **Section 111-23. Access to Covered Account Information.**

- (a) Access to customer accounts shall be password protected and shall be limited to authorized City personnel. Such password(s) shall be changed by the director of information technology or his designee on a regular basis, shall be at least 6 characters in length. Any unauthorized access to or other breach of customer accounts is to be reported immediately to the City Manager and the password changed immediately.
- (b) 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 111-24. Credit Card Payments.**

- (a) 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.
- (b) 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.
- (c) 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 111-25. 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 that may be received in the future by the City.* The City does not subscribe to or contract with any consumer reporting agency at this time.
- (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; or
- d. 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 or a phone number that is inconsistent with external or internal information sources used by the City.
- b. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer.
- c. Personal identifying information or a phone number or address, is associated with known fraudulent applications or activities as indicated by internal or external sources used by the City.
- d. Other information provided, such as fictitious mailing address, mail drop addresses, jail addresses, invalid phone numbers, or answering services, is associated with fraudulent activity.
- e. 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.
- f. 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.
- g. Personal identifying information is not consistent with personal identifying information that is on file with the City.

(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: 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:
  - 1. Nonpayment when there is no history of late or missed payments;
  - 2. 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 111-26. Prevention and Mitigation of Identity Theft.**

- (a) 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 Director of the Department of Utilities (“DDU”). If, in his or her discretion, such employee deems that identity theft is unlikely or that reliable information is available to reconcile red flags, the employee shall convey this information to Executive Assistant to the Director of the Department of Utilities (“EA”), who may in his or her discretion determine that no further action is necessary. If the EA in his or her discretion determines that further action is necessary, a City employee shall perform one or more of the following responses, as determined to be appropriate by the EA:
- (1) Contact the customer;
  - (2) Make the following changes to the account if, after contacting the customer, it is apparent that someone other than the customer has accessed the customer’s covered account:
    - a. change any account numbers, passwords, security codes, or other security devices that permit access to an account; or
    - b. close the account;
  - (3) Cease attempts to collect additional charges from the customer;
  - (4) Notify law enforcement, in the event that someone other than the customer has accessed the customer’s account causing additional charges to accrue or accessing personal identifying information; or
  - (5) Take other appropriate action to prevent or mitigate identity theft.
- (b) 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 to 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 DDU. If, in his or her discretion, such employee deems that identity theft is unlikely or that reliable information is available to reconcile red flags, the employee shall convey this information to the EA, who may

in his or her discretion determine that no further action is necessary. If the EA in his or her discretion determines that further action is necessary, a City employee shall perform one or more of the following responses, as determined to be appropriate by the EA:

- (1) Request additional identifying information from the applicant;
- (2) Deny the application for the new account;
- (3) Notify law enforcement of possible identity theft; or
- (4) Take other appropriate action to prevent or mitigate identity theft.

**Section 111-27. Updating the Program.**

The Mayor and 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 111-28. Program Administration.**

The DDU 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 types of covered accounts. Any recommended material changes to the program shall be submitted to the Mayor and City Council for consideration by the Council.

- (1) The DDU will report to the City Manager at least annually, on compliance with the red flag requirements.

- (2) The DDU and the EA are 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 DDU and the EA shall exercise their discretion in determining the amount and substance of training necessary.

### **Section 111-29. 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 DDU 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.

### **Section 111-30. Treatment of Address Discrepancies.**

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 111-31. Furnishing Consumer's Address to Consumer Reporting Agency.**

In the event that the City uses the services of a consumer reporting agency and 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:

- (1) The City is able to form a reasonable belief that the consumer report relates to the consumer about whom the City requested the report;
- (2) The City establishes a continuing relation with the consumer; and

- (3) 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.

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 111-32. 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.

**Section 111-33 – 111-54 . Reserved.**