ORDINANCE 02-2009

IDENTITY THEFT PREVENTION PROGRAM

AN ORDINANCE ESTABLISHING AN IDENTITY THEFT PREVENTION PROGRAM IN COMPLIANCE WITH REGULATIONS ISSUED BY THE FEDERAL TRADE COMMISSION.

WHEREAS, the Grand Rivers city council desires to comply with the identity theft prevention program regulations issued by the Federal Trade Commission,

BE IT ORDAINED by the city council of the City of Grand Rivers, Kentucky as follows:

Ordinance No. 02-2009 is hereby enacted and shall read in full as follows:

Sections:

I. PURPOSE

The purpose of this program is 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.

II. DEFINITIONS

1. "*City*" means the City of Grand Rivers, Kentucky.

2. "*Covered account*" means a utility account.

3. "*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.

4. "*Creditor*" means any person who regularly extends, renews, or continues credit, any person who regularly arranges for the extension, renewal, or continuation of credit, and any assignee of an original creditor who participates in the decision to extend, renew, or continue credit. This term shall include lenders such as banks, finance companies, automobile dealers, mortgage brokers, utility companies, and telecommunications companies.

5. "*Customer*" means a person who has a covered account with a creditor.

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

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

8. "*Service provider*" means a person who provides a service directly to the city.

III. PERSONAL IDENTIFYING INFORMATION MAY BE REQUIRED

As a precondition to opening a covered account in the city, each applicant may be required to provide the city with personal identifying information such as a valid government issued identification card containing a photograph of the applicant. The authorized city personnel processing the application for a covered account shall determine in his/her discretion whether personal identifying information shall be provided by the applicant.

IV. ACCESS TO COVERED ACCOUNT INFORMATION

Access to customer accounts shall be limited to authorized city personnel. Any unauthorized access to or other breach of customer accounts is to be reported immediately to the City Clerk.

V. 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. Such red flags may include, but are not limited to, the following:

1. Alerts from consumer reporting agencies, fraud detection agencies, or service providers.

2. Suspicious documents.

   Examples of suspicious documents may include, but are not limited to the following:

   (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 city; 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 personal identification may include, but are not limited to the following:

(a.) Personal identifying information, phone number, or address is associated with known fraudulent applications or activities as indicated by internal or third-party sources used by the city.

(b.) 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.

(c.) 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.

(d.) 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.

(e.) Personal identifying information is not consistent with personal identifying information that is on file with the city.

(f.) 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 may include, but are not limited to the following:

(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.) An account is used in a manner that is not consistent with established patterns of activity on the account. For example, there is nonpayment when there is no history of late or missed payments.

(c.) An account that has been inactive for a long period of time is used.

(d.) Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's account.

(e.) The city is notified of unauthorized charges or transactions in connection with a customer's account.

5. Notice from customers, law enforcement, victims, or other reliable sources regarding possible identity theft.

VI. PREVENTION AND MITIGATION OF IDENTITY THEFT

1. New Account

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/her discretion to determine whether such red flag or combination of red flags suggests a threat of identity theft. If such employee determines that identity theft or attempted identity theft is likely or probable, such employee shall immediately report such red flags to the City Clerk. The City Clerk shall determine whether to do one or more of the following:

(a.) Request additional identifying information from the applicant.

(b.) Deny the application for the new account.

(c.) Notify law enforcement.

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

2. Existing Account

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/her discretion to determine whether such red flag or combination of red flags suggests a threat of identity theft. If such employee determines that identity theft or attempted identity theft is likely or probable, such employee shall immediately report such red flags to the City Clerk. The City Clerk shall determine whether to do one or more of the following:

(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 accessed 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.) Notify law enforcement.

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

VII. UPDATING THE PROGRAM

The City Clerk shall annually review and, as deemed necessary by the City Clerk, recommend to the city council updates to 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 doing so, the City Clerk shall consider the following factors:

(a.) The city's experiences with identity theft.

(b.) Updates in methods of identity theft.

(c.) Updates in customary methods used to detect, prevent, and mitigate identity theft.

(d.) Updates in the types of accounts that the city offers or maintains.

(e.) Updates in service provider arrangements.

VIII. PROGRAM ADMINISTRATION

The City Clerk is responsible for oversight of the program and for program implementation. The City Clerk is responsible for distributing a copy of the Identity Theft Prevention Program 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.

IX. OUTSIDE SERICE 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/her discretion in reviewing such arrangements in order to reasonably ensure that the service provider's activities 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.

X. SEVERABILITY

Each section and each provision of each section of this ordinance are severable, and if any provision, section, paragraph, sentence, or part thereof, or the application thereof to any person, licensee, class, or group is held by a court of law to be unconstitutional or invalid for any reason, such holding shall not affect or impair the remainder of this ordinance, it being the legislative intent to ordain and enact each provision, section, paragraph, sentence, and part thereof separately and independently of the rest.

XI. EFFECTIVE DATE

This ordinance shall be effective immediately upon its publication.

Date of First Reading of Ordinance: March 10, 2009

Date of Second Reading of Ordinance: April 14, 2009

Date of Publication of Ordinance: April 28, 2009

Ordinance Published in: Livingston Ledger

B. T. Moodie, Mayor

ATTEST:

Joe Dry, City Clerk

Certification

I, Joe Dry, do hereby certify that I am the duly appointed clerk of the City of Grand Rivers, Kentucky, that the foregoing Ordinance is a true and correct copy of the ordinance duly adopted at a meeting of the City Council on April 14, 2009 that this Ordinance is in the form presented to said meeting and in the form executed, and the said ordinance appears as a matter of public record in the Official City Ordinance Book and is still in full force and effect.

IN TESTIMONY WHEREOF, witness my signature on this 14th day of April, 2009.

Joe Dry, City Clerk

EMPLOYEE/OFFICER ACKNOWLEDGEMENT

I _____ [*printed name*] have received a copy of the Identity Theft Prevention Program. I have read the Identity Theft Prevention Program. I agree to abide by all terms of the Identity Theft Prevention Program.

_____

EMPLOYEE/OFFICER

_____

DATE