

Town of Georgetown, IN

Ordinance # G-09-03

An Ordinance Adopting the Town of Georgetown Red Flag Compliance And Identity Theft Prevention Policy

BE IT ORDAINED BY THE TOWN COUNCIL OF THE TOWN OF GEORGETOWN, INDIANA THAT:

WHEREAS, pursuant to federal law the Federal Trade Commission (FTC) adopted the 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 FTC 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 FTC regulations include utility companies in the definition of creditor;

WHEREAS, the Town of Georgetown ("Georgetown") is a creditor with respect to 16 CFR § 681.1 by virtue of providing utility services or by otherwise accepting payment for municipal services in arrears;

WHEREAS, the FTC 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 FTC 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;

WHEREAS, the duly elected governing body of Georgetown is the Georgetown Town Council;

**NOW BE IT THEREFORE ORDAINED THAT THE TOWN OF GEORGETOWN
ADOPTS THE RED FLAG COMPLIANCE AND IDENTITY THEFT PREVENTION
PROGRAM ATTACHED HERTO AS EXHIBIT "A" AND MADE A PART HEREOF**

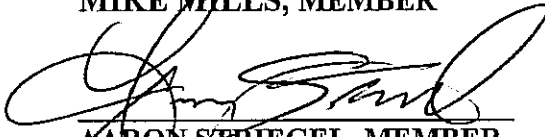
Adopted by the Town Council of the Town of Georgetown, Indiana, this 13 day of April, 2009.



BILLY STEWART, PRESIDENT



MIKE MILLS, MEMBER



AARON SPIEGEL, MEMBER



EVERETT PULLEN, MEMBER



KARLA PERKINS, MEMBER

ATTEST:



DOUGLAS COOK, CLERK/TREASURER

EXHIBIT "A"

RED FLAG POLICY

TOWN OF GEORGETOWN RED FLAG COMPLIANCE
AND IDENTITY THEFT PREVENTION POLICY

Section 1 – Short Title

This article shall be known as the Red Flag Compliance Program

Section 2. - 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 3. - Definitions.

For the purposes of this Article, the following definitions apply:

“Town” means Town of Georgetown

“Covered Account” means (i) An account that a 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, 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.

“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 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.

“Customer” 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.

“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 Town.

Section 4. - Process of Establishing a Covered Account

As a precondition of opening a covered account with the Town, each applicant shall provide the Town with the following information:

- a. The customer’s name
- b. The customer’s billing address
- c. The property address (if applicable)
- d. The customer’s phone number
- e. A customer may set up an automatic bank withdrawal by filing out a request form for an automatic bank withdraw

Section 5. – Access to Covered Account Information

- a. Access to customer accounts shall be password protected or kept in a locked filing cabinet and shall be limited to authorized Town personnel.
- b. All account sensitive customer account information such as bank account numbers or routing numbers shall be stored in a secure computer system which is password protected.
- c. Any unauthorized access to or other breach of customer accounts is to be reported immediately to the Clerk/Treasurer and the password changed immediately.
- d. Personal identifying information included in customer accounts is considered confidential and any request or demand for such information shall immediately forwarded to the Clerk/Treasurer and the Town Attorney.

Section 6. - Credit Card Payments

The Town shall not take any payment by credit or debit card. Neither shall the Town collect or ask for credit or debit card information.

Section 7. – 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:

Suspicious Documents. Examples of suspicious documents include:

- a. Documents provided for identification that appear to be forged or altered.
- b. Identification on which the photograph or physical description is inconsistent with the appearance of the applicant or customer.
- c. Identification which is inconsistent with information readily accessible on file with the Town.

Suspicious personal identification

- a. Inconsistent personal information.
- b. Lack of personal information beyond that which generally would be available from a wallet or consumer report.

Unusual or suspicious activity relating to a covered account.

- a. Customer fails to make first payment or makes an initial payment but no subsequent payments.
- b. Mail sent to the customer is returned although transactions continue to be conducted in connection with the customer's account.
- c. Suspicious inquiries about covered account information by any person, including persons representing themselves to be the account holder or the account holder's representative.
- d. The Town is notified of unauthorized charges or transactions in connection with a customer's account.
- e. The Town is notified by a customer, law enforcement or another person that a fraudulent account has been opened for a person engaged in identity theft.

Section 8. - Prevention and Mitigation of Identity Theft.

In the event that any Town 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