

RESOLUTION R-2009-21
A RESOLUTION ADOPTING AN IDENTITY THEFT POLICY AND DECLARING
AN EMERGENCY

WHEREAS, the Federal Fair and Accurate Credit Transaction Act of 2003, which is an amendment to the Fair Credit Reporting Act, has established rules requiring identity theft protection to be promulgated by creditor institutions; and

WHEREAS, these rules are administered by the Federal Trade Commission; and

WHEREAS, the Federal Trade Commission has determined that any business, including municipal utilities and other municipal departments are to be treated as creditor institutions in the event the municipality does not require payment in advance for utilities being provided; and

WHEREAS, the Council of the Village of Windham has determined that an Identity Theft Policy is in the best interest of the municipality and its citizens.

NOW, THEREFORE, BE IT RESOLVED, by the Council of the Village of Windham, Portage County, Ohio, two thirds or more of the members thereto concurring that:

SECTION 1: The Identity Theft Policy attached hereto as Exhibit "A" and incorporated herein by reference, is hereby established by the Council of Windham to govern all utility and credit transactions with the Village.

SECTION 2: It is hereby found and determined that all formal actions of this Council concerning and relating to the adoption of this Resolution were adopted in an open meeting of this Council and that all the deliberations of the Council and any of its committees that resulted in such formal action were in meetings open to the public in compliance with all legal requirements including Section 121.22 of the Revised Code of the State of Ohio.

SECTION 3: This Resolution is hereby declared to be an emergency measure, effective immediately upon its passage, for the preservation of the public health, safety and welfare within the whole of the Village and to comply with the Federal Trade Commission requirements to have an Identity Theft Policy must be in place as soon as possible.

First Reading, passed as an Emergency this 23rd day of June, 2009.

Vote of Council: Ayes: Mr. Snyder, Mr. Garrett, Mrs. Barrett, Mrs. Meszaros, Mrs. Rininger, Mr. Slusher. Nays: None.

Adopted: June 23, 2009

Approved: _____

Effective: June 23, 2009

By: _____
Robert W. Donham, II, Mayor

Attest:

Fiscal Officer, Lloyd Billman

Approved as to form:

Village Solicitor, Thomas Reitz

EXHIBIT "A"
Resolution R-2009-21

Identity Theft Prevention Program
For
Village of Windham
9621 East Center Street
Windham, Ohio 44288
June 17, 2009

Village of Windham Identity Theft Prevention Program

This Program is intended to identify red flags that will alert our employees when new or existing accounts are opened using false information, protect against the establishment of false accounts, methods to ensure existing accounts were not opened using false information, and measures to respond to such events.

Contact Information:

The Management Person responsible for this program is:

Name:

Title:

Phone number:

The Village Council as of the date this Program was enacted are:

1. Phil Snyder
2. Rachel W. Baret
3. Kelly Meszaros
4. Scott Garrett
5. Randy Slusher
6. Linda Rininger

Risk Assessment

The Village of Windham has conducted an internal risk assessment to evaluate how at risk the current procedures are at allowing customers to create a fraudulent account and evaluate if current (existing) accounts are being manipulated. This risk assessment evaluated how new accounts were opened and the methods used to access the account information. Using this information the Village was able to identify the following red flags that are appropriate to prevent identity theft:

- New accounts opened In Person.
- Account information accessed In Person.
- Account information accessed via Telephone (Person)

Detection (Red Flags):

The Village of Windham here by adopts the following red flags to detect potential fraud. These are not intended to be all-inclusive and other suspicious activity may be investigated as necessary:

- Identification documents appear to be altered.
- Photo and physical description do not match appearance of applicant.
- Other information is inconsistent with information provided by applicant
- Other information provided by applicant is inconsistent with information on file.
- Application appears altered or destroyed and reassembled.

- ❑ Personal information provided by applicant does not match other sources of information (e.g. credit reports, SS# not issued or listed as deceased)
- ❑ Information provided is associated with known fraudulent activity (e.g. address or phone number provided is same as that of a fraudulent application).
- ❑ Information commonly associated with fraudulent activity is provided by applicant (e.g. address that is a mail drop or prison, non-working phone number or associated with answering service/pager)
- ❑ SS#, address, or telephone # is the same as that of other customer at utility
- ❑ Customer fails to provide all information requested.
- ❑ Personal information provided is inconsistent with information on file for a customer.
- ❑ Applicant cannot provide information requested beyond what could commonly be found in a purse or wallet
- ❑ Identify theft is reported or discovered

Response

Any employee that may suspect fraud or detect a red flag will implement the following response as applicable. All detections or suspicious red flags shall be reported to the designated management official:

- ❑ Ask applicant for additional documentation
 Notify internal manager: Any utility employee who becomes aware of a suspected or actual fraudulent use of a customer or potential customers identity must notify the Village Administrator.
- ❑ Notify law enforcement: The utility will notify Windham Police Chief at Windham Police Department of any attempted or actual identity theft.
- ❑ Do not open the account

Personal Information Security Procedures:

The Village of Windham hereby adopts the following security procedures.

1. Files containing personally identifiable information are kept in locked file cabinets except when an employee is working on the file.
2. Employees will not leave sensitive papers out on their desks when they are away from their workstations.
3. Anti-virus and anti-spyware programs will be run on individual computers and on servers daily.
4. Computer passwords will be required.

5. Passwords will not be shared or posted near workstations.
6. The computer network will have a firewall where your network connects to the Internet.
7. Check references or do background checks before hiring employees who will have access to sensitive data.
8. New employees sign an agreement to follow your company's confidentiality and security standards for handling sensitive data.
9. Access to customer's personal identity information is limited to employees with a "need to know".
10. Employees will be alert to attempts at phone phishing.
11. Employees who violate security policy are subjected to discipline, up to and including, dismissal.
12. Paper records will be shredded before being placed into the trash.

Identity Theft Prevention Program Review and Approval

This plan has been reviewed and enacted by the Council of the Village of Windham Council by Resolution R-2009-21, passed by Council on the _____ day of _____, 2009.