

**RESOLUTION 44-2008**

**A RESOLUTION OF THE TOWN OF MALABAR, ADOPTING A  
IDENTITY THEFT PREVENTION PROGRAM POLICY PROTECTING  
AGAINST THE ESTABLISHMENT OF FALSE ACCOUNTS;  
PROVIDING FOR METHODS TO ENSURE EXISTING ACCOUNTS ARE  
NOT OPENED USING FALSE INFORMATION; PROVIDING  
MEASURES TO RESPOND TO SUCH EVENTS; PROVIDING AN  
EFFECTIVE DATE.**

**WHEREAS**, the “Red Flag” anti-identity theft rules were adopted under the Fair and Accurate Credit Transactions Act of 2003 (“FACTA”) and stated November 1, 2008 as the deadline for compliance by utility departments and others; and

**WHEREAS**, the “Red Flag” rule applies to Malabar in respect to the utility account set up for each customer and the required information that must be provided; and

**WHEREAS**, the rules were issued jointly by various federal agencies and require adoption of a policy by the Town Council.

**NOW, THEREFORE, BE IT RESOLVED BY THE TOWN OF MALABAR:**

**Section 1.** That the Town of Malabar adopts the attached Identity Theft Prevention Program Policy as Exhibit “A”

**Section 2.** That a copy of this resolution shall be provided to the Malabar Utility Department.

**Section 3.** This Resolution shall take effect immediately upon its adoption.

This Resolution was moved for adoption by Council Member McClelland. This motion was seconded by Council Member Vail and, upon being put to vote, the vote was as follows:

Council Member Nancy Borton	<u>Aye</u>
Council Member Brian Vail	<u>Aye</u>
Council Member Charles (Chuck) McClelland	<u>Aye</u>
Council Member Jeffrey (Jeff) McKnight	<u>Aye</u>
Council Member Patricia D. Dezman	<u>Aye</u>

This Resolution was then declared to be duly passed and adopted this 20th day of October, 2008.

By: Thomas Eschenberg  
Mayor Thomas M. Eschenberg  
Town of Malabar

Approved as to form and content:

*Karl Bohne*

Karl W. Bohne, Jr., Town Attorney

ATTEST:

*Debby Franklin*

Debby K. Franklin  
Town Clerk/Treasurer

(seal)

## EXHIBIT "A"



**PROCEDURE NUMBER: 2008-01**

**SUBJECT TITLE: Identity Theft Prevention Program Policy**

**EFFECTIVE DATE: 11/01/2008**

**DISTRIBUTION: ADMINISTRATIVE STAFF IN TOWN HALL**

**RESCINDS: N/A**

**POLICY:**

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, provide methods to ensure existing accounts are not opened using false information and measures to respond to such events.

The Senior Management Person responsible for this program is the Town Clerk/Treasurer:

**Risk Assessment:**

The Town of Malabar Utility Department 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 utility department was able to identify red flags that were appropriate to prevent identity theft on the following:

- New accounts opened In Person
- New accounts opened via Fax
- Account information accessed In Person
- Account information accessed via Telephone (Person)
- Account information accessed via Fax
- Identity theft occurred in the past from someone falsely using a current account or falsely opening a utility account

**Detection (Red Flags):**

The Town of Malabar Utility Department has adopted 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.
- Information provided is associated with known fraudulent activity (e.g. address or phone number provided is same as that of a fraudulent application)
- SS#, address, or telephone # is the same as that of other utility customer
- 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
- Identity 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 Town Clerk/Treasurer immediately upon detection.

- ✚ Ask applicant for additional documentation
- ✚ Notify supervisor: Any utility employee who becomes aware of a suspected or actual fraudulent use of a customer or potential customers' identity must notify the Town Clerk or a designee
- ✚ Notify law enforcement: The Utility Department will notify the Brevard County Sheriff's Office of any attempted or actual identity theft
- ✚ Do not open the account
- ✚ Close the account
- ✚ Do not attempt to collect against the account, but notify authorities

**Personal Information Security Procedures:**

The Town of Malabar Utility Department adopted the following security procedures:

1. Paper documents, files, and electronic media containing secure information will be stored in locked file cabinets after business hours. File cabinets will be stored in a locked area.
2. Only specially identified employees with a legitimate need will have access to the keys to the room and cabinet. Keys are kept in the safe except when locking or unlocking the file cabinet.
3. Files containing personally identifiable information are kept in locked file cabinets except during work hours when an authorized employee is always present.

4. Employees will not leave uncovered sensitive papers out on their desks when they are away from the area of their workstations.
5. Employees store sensitive files in locked file cabinets when leaving their work areas at the end of the day.
6. Employees lock their computers when leaving their work areas.
7. Employees keep access to the utility billing area locked at all times.
8. Access to offsite storage facilities is limited with access keys in possession of Town Clerk.
9. Visitors who must enter areas where sensitive files are kept must be escorted by an employee of the utility department.
10. No visitor will be given any entry codes/cards or allowed unescorted access to the office.
11. Passwords will not be shared or posted near workstations.
12. Sensitive information that is sent to third parties over public networks will be encrypted.
13. When sensitive data is received or transmitted, secure connections will be used.
14. Computer passwords will be required.
15. User names and passwords will be different.
16. Anti-virus and anti-spyware programs will be run on servers daily.
17. The computer network will have a firewall where your network connects to the Internet.
18. Check references or do background checks before hiring employees who will have access to sensitive data.
19. Procedures exist for making sure that workers who leave our employ or transfer to another part of the company no longer have access to sensitive information.

**Annual Report:**

A report will be prepared annually and submitted to the Town Clerk/Treasurer or a designee above to include matters related to the program, the effectiveness of the policies and procedures, the oversight and effectiveness of any third party billing and account establishment entities, a summary of any identify theft incidents and the response to the incident, and recommendations for substantial changes to the program, if any.