ATTACHMENT A

A RESOLUTION ADOPTING AN
IDENTITY THEFT/RED FLAG RULES POLICY AND PROCEDURES
Resolution No. 102/2008-09

WHEREAS, the Federal Trade Commission (FTC) has required that all financial institutions and creditors who establish or maintain "covered accounts" containing customer "identifying information" as defined by the Fair and Accurate Credit Transactions Act (FACTA) of 2003 establish identity theft protection programs; and

WHEREAS, the Town of Carrboro has evaluated accounts maintained by the Town, as to their type and vulnerability to identity theft, for the purpose of identifying applicability to the FACTA regulations;

NOW, THEREFORE, BE IT RESOLVED, that the Board of Aldermen of the Town of Carrboro concurs with the staff evaluation and adopts the Identity Theft/Red Flag Rules Policies and Procedures for the Town of Carrboro.

This resolution shall become effective upon adoption.

IDENTITY THEFT/RED FLAG RULES POLICY AND PROCEDURE

Town of Carrboro
Board of Aldermen

Prepared by: Nancy H. B. Emslie
Accounting Officer

Introduction

In 2003, Congress passed the Fair and Accurate Credit Transactions Act (FACT Act) to address the increasing problems with identity theft and misuse of personal information of consumers. In November 2007, the final rules (known as the ***Red Flag Rules***) and guidelines were issued to implement the FACT Act with an effective date of January 1, 2008 and with full compliance required by November 1, 2008. In October 2008 the Federal Trade Commission (FTC) suspended mandatory enforcement of the new "Red Flag Rule" until May 1, 2009 to give financial institutions and creditors additional time to develop and implement written identity theft prevention programs.

The regulations, known as the *identity theft "red flag"* rules, require the entities they cover to develop policies and procedures to recognize and respond to circumstances that may indicate identity theft has occurred for both new and existing accounts. The new set of regulations is intended to help prevent, detect, and respond to possible signals (red flags) to mitigate identity theft.

The rules apply to financial institutions and *creditors* (a term that is defined to include any government agency that "regularly extends, renews, or continues *credit*") who establish or maintain *covered accounts* containing customer *identifying information* as defined by the FACT Act of 2003. These rules also apply to local governments when they provide a service for which payment is deferred until a future date.

This policy is being initiated in order for the Town of Carrboro to comply with three (3) new FACT Act regulations referred to as the ***Red Flag Rules***, section 114 and 315 of the FACT Act. The FTC's portion of the rules is contained in Part 681 of Title 16 of the Code of Federal Regulations.

Purpose

The purpose of this policy is to identify programs and services (accounts) where information is collected by the Town from citizens in a "creditor" relationship, determine whether such information is maintained in "covered accounts" containing customer "identifying information" per federal regulations, and establish procedures for the security of such information if necessary.

Definitions

- **Covered Account** – 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; or 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** –The right granted by a creditor to defer payment or debt or to incur debts and defer its payment or to purchase property or services and defer payment therefore.

- **Creditor** – Any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation or credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit.

- **Identifying Information** –Any name or number that may be used, alone or in connection with any other information, to identify a specific person, including any:

    1. Name, address, telephone number, social security number, date of birth, official state or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;
    2. Unique biometric data, such as fingerprint, voiceprint, retina or iris image, or other unique physical representation;
    3. Unique electronic identification number, address or routing code; or
    4. Telecommunication identifying information or access device.

- **Identity Theft** – Fraud committed using the identifying information of another person.

- **Notice of Address Discrepancy**- Notifies the user of a substantial difference between the address the user provided and the address in the nationwide wide consumer reporting agency (NCRA).

- **Red Flag** – A pattern, practice, or specific activity that indicates the possible existence of identity theft.

Accounts

(a) Assessments—The Town may, from time to time, apply assessments to property owners for the purpose of recovering some or all of the costs of a variety of improvements. Per the definitions listed above, the Town acts as a creditor maintaining a covered account. Accounts established and maintained of property owners owing assessments do not contain any identifying information that is not public information and obtained from Orange County property tax records. Thus, the regulations of Fair and Accurate Credit Transactions Act (FACTA) do not apply.

(b) Inspection and Permit Fees – The Town imposes inspection and permit fees for the general purpose of consumer services. These types of fees are considered a one-time fee which is paid upfront and is not deferred until a future date. No accounts are established by the Town that allow for multiple payments or transactions. .Records kept may include the following identifying information: a person's name, business name, address, telephone number, state license number or the Town's privilege license number. Since an account is not maintained nor is the fee considered a multiple payment or transaction, for these reasons, the regulations of FACTA do not apply.

(c) Privilege License Fees – The Town imposes a license tax for the privilege of conducting business in the Town. This is an annual fee which is paid upfront and is not deferred until a future date. Records kept may include the following identifying information: a person's name and social security or taxpayer identification number, depending on the type of business, address or telephone number. The Town does not act as a creditor for these accounts; therefore, the regulations of FACTA do not apply.

(d) Property Taxes – The Town receives revenue from the collection of property taxes. Tax billing and collection services are provided for the Town by the Tax Collection offices of Orange County, in establishing and maintaining ad valorem taxes and accounts for customers. To the Town's knowledge such accounts established and maintained of property owners owing taxes and fees do not contain any identifying information that is not public information and readily obtained "on line" from the Orange County property tax records. The Town does not directly collect ad valorem taxes and/or fees, or maintain accounts regarding the same, or have access to, any identifying information as defined hereinabove and, thus, the regulations of FACTA do not apply.

(e) Recreation Fees – The Town charges recreation fees for various programs and services offered by the town. Many of these types of payments received are considered a one-time fee which is paid upfront. However, regarding facility rentals, the Town requests a 10% non-refundable pre-payment and invoices the balance due to be paid prior to the rental date. Summer Camp offers a payment plan to those registering, while softball teams may elect to place a deposit upon registering with the balance due by a specified time. Records kept may include the following identifying information: a person's name, business name, date of birth, address or telephone number. The Town does act as a creditor and the recreation fees could be considered a covered account; therefore, the regulations of FACTA do apply.

(f) Revolving Loan – The Town offers revolving loans to private non-profit and for-profit firms for projects resulting in the creation or retention of jobs. The revolving loan fund also provides the community with a source of financing to undertake economic development activities. Every applicant is required to complete an application which includes a copy of their credit report. The application is reviewed through a formal review process. Funded loans are repaid with multiple payments or transactions. The

Town does act as a creditor and the revolving loans could be considered a covered account; therefore, the regulations of FACTA do apply.

(g) Solid Waste and Recycling Dumpster Fees – The Town charges fees for the collection of garbage from dumpsters; therefore, billing services are provided by the Town. The solid waste and recycling dumpsters are, however, primarily for businesses and not family or household customers. Records kept may include the following identifying information: a person's name and social security or taxpayer identification number, depending on the type of business, and an address and telephone number. Since the aforementioned service is not primarily provided to families or households, the regulations of FACTA do not apply.

Procedures

1) Managing, maintaining, and storing sensitive and confidential information

(a) Employees who have access to sensitive and confidential information are required to create, handle, maintain, and dispose of such information with prudent care in order to ensure proper security. Access to sensitive and confidential information will be limited and only provided in order for authorized employees and contractual third parties to perform essential tasks for Town business.

(b) The following procedures should be followed while creating, handling, maintaining, storing, and disposing of sensitive information.

1. Enter information directly to a final destination (i.e. computer system) and refrain from documenting the information in other areas.
2. Sensitive information should not be included on e-mails.
3. Sensitive information should not be included on printed reports except as needed for the performance of essential tasks.
4. Maintain documents that contain sensitive information in a secured area and limit access to the area.
5. If possible, utilize encryption to secure information in the database or storage system.
6. Do not leave a computer unattended if sensitive information could be accessed by unauthorized individuals. While away from the computer, log off or lock the workstation.
7. Do not store files with sensitive information on laptops or on flash drives unless the information and the device can be secured and not accessible to unauthorized individuals.
8. Take reasonable measures when destroying sensitive data that will prohibit the information from being read or reconstructed. Documents with sensitive data should be shredded by the individual who has authorized

access to the data or by another employee while in the presence of the authorized employee. The Town may enter into a written contract with a third party in the business of record destruction to destroy sensitive information in a manner consistent with this policy.

(c) In order to protect sensitive and confidential information, the Town will only release sensitive information to the account holder or individual(s) who own the information upon confirmation of personal identifying information or a valid picture ID. The confirmed account holder or individual may authorize the release of sensitive information to a third party. Confidential information will only be released in accordance with state statute. The only exception will be the release of specified information pursuant to a court order, warrant, subpoena or other requirement by law.

2) Identification of Red Flags

The Red Flags rule defines "Identity Theft" as "fraud" using "identifying information" of another person. "Identifying information" includes: name, address, telephone number, social security number, date of birth, government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, unique electronic identification number, computer's internet protocol address, routing code.

In order to identify relevant Red Flags, the Town considers the types of accounts that it offers and maintains, the methods it provides to open its accounts, the methods it provides to access its accounts, and any previous experiences with Identity Theft.

(a) Step 1. Employees shall be aware of the following "Red Flags" that suggest a breach of sensitive or confidential information has occurred.

1. Physical Breach - The following are indications that there has been unauthorized access to sensitive and confidential information via a physical breach. Other activities may occur that are also physical breaches that are not included in the listing.
    a. Evidence of lock tampering on file cabinets or office doors.
    b. Evidence of unauthorized entry in an area where sensitive and confidential information is stored.
    c. Missing files or documents that contain sensitive information.

2. Technology Breach - The following are indications that there has been unauthorized access to sensitive and confidential information via a technology breach. Other activities may occur that are also technological breaches that are not included in the listing.
    a. Unknown or unauthorized name in the computer logon window.

b. Disconnected computer cables or power cables.
c. Missing computer equipment (desktop, laptop).
d. Evidence that electronic files have been accessed by unknown or unauthorized individuals or are missing.
e. Devices or media attached to the computer that are not known or authorized.
f. Unusual programs running, icons, or windows that appear that are not known and are not part of the normal work process.
g. Any other suspicious activity which indicates an attempt to use technology without approval.

3. Suspicious Documents. The following are indications that there has been unauthorized access to sensitive and confidential information from physical documents provided by third parties. Other activities may occur that are also breaches that are not included in the listing.

a. Identification document or card that appears to be forged, altered or inauthentic.
b. Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document.
c. Other document with information that is not consistent with existing customer information (such as if a person's signature on a check appears forged).
d. Application for service that appears to have been altered or forged.

4. Suspicious Personal Identifying Information. The following are indications that persons may be attempting to create or use fictitious identities. Other activities may occur that are also breaches that are not included in this listing.

a. Identifying information presented that is inconsistent with other information the customer provides (example: inconsistent birth dates),
b. Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a credit report).
c. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent.
d. Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address).
e. An address or phone number presented that is the same as that of another person.
f. A person fails to provide complete personal identifying information on an application when reminded to do so.

g. A person's identifying information is not consistent with the information that is on file for the customer.

5. Suspicious Account Activity or Unusual Use of an Account. The following are indications that persons may be attempting to create or use fictitious accounts. Other activities may occur that are also breaches that are not included in this listing.

   a. Change of address for an account followed by a request to change the account holder's name.
   b. Payments stop on an otherwise consistently up-to-date account.
   c. Account used in a way that is not consistent with prior use. (example: very high activity)
   d. Mail sent to the account holder is repeatedly returned as undeliverable.
   e. Notice to the Town that a customer is not receiving mail sent by the Town.
   f. Notice to the Town that an account has unauthorized activity.
   g. Breach in the Town's computer system security.
   h. Unauthorized access to or use of customer account information.

6. Alerts from Others. Notice to the Town from a customer, identity theft victim, law enforcement or other person that it has opened or is maintaining a fraudulent account for a person engaged in Identity Theft. An example of an alert could be a "*notice of address discrepancy*" from a nationwide consumer reporting agency (NCRA).

(b) Step 2. Detection of Red Flags.

1. New Accounts. In order to detect any of the red flags identified above associated with the opening of a new account, employees shall take the following steps to obtain and verify the identity of the person opening the account:

   a. Require certain identifying information such as name, date of birth, residential or business address, principal place of business for an entity, driver's license or other identification.
   b. Verify the customer's identity (for instance, review a driver's license or other identification card).
   c. Review documentation showing the existence of a business entity.
   d. Independently contact the customer if the application is not made in person by the customer.

2. Existing Accounts. In order to detect any of the red flags identified above for an existing account, employees shall take the following steps to monitor transactions within an account:

    a. Verify the identification of customers if they request information (in person, via telephone, via facsimile, via email).
    b. Verify the validity of requests to change billing addresses.
    c. Verify changes in banking information given for billing and payment purposes.

3. Notice of Address Discrepancy. In order to detect any of the red flags identified regarding a Notice of Address Discrepancy, employees shall take the following steps:

    a. Compare information in the consumer report to information the user (1) maintains in its records; (2) obtains from third-party sources; and (3) obtains to comply with consumer information program rules.
    b. Verify information in the consumer report with the customer.
    c. Form a reasonable belief that the consumer report relates to the customer about whom it has requested the report, when the user receives a notice of address discrepancy.
    d. Notify the credit reporting agency that provided the Notice of Address Discrepancy of the Town's findings (whether the person at issue is in fact the same person about whom the discrepancy notice was received.)

(c) Step. 3. Responding to Red Flags—Preventing and Mitigating Theft.

In the event personnel detect any identified Red Flags, such personnel shall take one or more of the following steps, depending on the degree of risk posed by the Red Flag:

1. Internal notification. – Any Town employee who becomes aware of a suspected or actual security breach must notify his or her immediate supervisor. The immediate supervisor will notify department management who is responsible for further investigation, notification, and remediation.

2. External notification. – The Town is required to notify affected individuals of *actual* security breaches. Each suspected breach will be reviewed by the department where the breach occurred and then, with the Town Manager or his/her designee, determine appropriate action to include the following:

    a. Notify the affected individuals without unreasonable delay providing information in general terms about the incident, the type of sensitive information that was subject to the unauthorized access, the

actions that the Town will take to protect the information from further access.

b. Notice to affected individuals may be provided by one or more of the following methods:

i. Written notice.
ii. Telephonic notice provided the contact is made directly with the affected persons and appropriately documented by the Town.

3. Preventing and Mitigating Identity Theft

In the event employees identify the possibility of a red flag or identity theft, they shall take one or more of the following steps, depending on the degree of risk posed by the red flag:

a. Continue to monitor an account for evidence of Identity Theft.
b. Contact the customer.
c. Change any passwords or other security devices that permit access to accounts.
d. Not open a new account.
e. Close an existing account.
f. Reopen an account with a new number.
g. Notify the Finance Officer for determination of the appropriate step(s) to take.
h. Notify law enforcement.
i. Determine that no response is warranted under the particular circumstances.

4. Protection of Confidential Information

In order to further prevent the likelihood of identity theft occurring with respect to Covered Accounts, the Town will take the following steps with respect to its internal operating procedures to protect confidential information:

a. Ensure that its website is secure or provide clear notice that the website is not secure.
b. Ensure complete and secure destruction of paper documents and computer files containing customer information.
c. Ensure that office computers are password protected and that computer screens lock after a set period of time.
d. Keep offices clear of papers containing customer information.
e. Request only the last 4 digits of social security numbers (if any).

f. Ensure computer virus protection is up to date.
g. Require and keep only the kinds of customer information that are necessary for Town purposes.

5. Program Updates

This Policy and Plan shall be reviewed and updated annually to reflect changes in risks to customers and the soundness of the Town from Identity Theft. The Finance Officer or his/her designee shall consider the Town's experiences with Identity Theft situations, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, changes in types of accounts the Town maintains and changes in the Town's business arrangements with other entities. After considering these factors, the Finance Officer or his/her designee will determine whether changes to the Policy or Plan are warranted. If warranted, the Finance Officer or his/her designee will update the Policy or Plan and present the Board of Aldermen with recommended changes and the Board of Aldermen will make a determination as to whether to accept, modify or reject those changes to the Policy.

I. Program Administration

a. Oversight - Responsibility for developing, implementing and updating this Policy lies with the Finance Officer or his designee. The Finance Officer may create an Identity Theft Committee at his/her discretion. If created, the Committee shall be chaired by the Finance Officer or his/her designee. Two or more other individuals appointed by Finance Officer shall comprise the remainder of the committee. The Identity Theft Committee shall be responsible for the Policy administration, for ensuring appropriate training of employees on the Policy, for reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating Identity Theft, determining which steps of prevention and mitigation should be taken in particular circumstances and considering periodic changes to the Policy or Plan.

b. Staff Training and Reports - Employees with access to Covered Accounts shall be trained and made aware of this Policy and Plan. The Finance Officer or his/her designee may require reports from such employees at his/her discretion.

c. Service Provider Arrangements - In the event the Town engages a service provider to perform an activity in connection with one or more Covered Accounts, the Town will take the following steps to ensure the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of Identity Theft.

1. Require, by contract, that service providers have such policies and procedures in place.

2. Require, by contract, that service providers review the Town's Policy and Plan and report any red flags to the Finance Officer, his/her designee, or the Identity Theft Committee.

d. Specific Program Elements and Confidentiality - This Policy and Plan requires a significant degree of confidentiality regarding the Town's specific practices relating to Identity Theft detection, prevention and mitigation. Therefore, under this Policy, knowledge of such specific practices are to be limited to only those employees who need to know them for purposes of preventing Identity Theft.

Conclusions

A complete assessment of the Town's accounts revealed that the Town is considered a "creditor" and does maintain "covered accounts" for its Revolving Loan Program and for Recreation and Park fees collected.

The Town will implement the aforementioned systems and procedures to help ensure the confidentiality of financial transactions associated with these types of activities.

This policy will be reviewed annually by the Finance Officer or his/her designee or the Identify Theft Committee (if created). Recommended updates that reflect changes in accounts and services, or its relationship with customers will be brought back to the Board of Aldermen for approval.