First Reading: 04/27/09
Second Reading: 05/11/09
Third Reading: 06/08/09
Public Hearing: 06/08/09

SC Act 190 and FACT Act Ordinance
May 2009

COUNTY OF FAIRFIELD, SOUTH CAROLINA

ORDINANCE NO. 547

TO ESTABLISH AN IDENTITY THEFT PREVENTION PROGRAM; TO COMPLY WITH FEDERAL REGULATIONS RELATING TO ADDRESS DISCREPANCIES; TO COMPLY WITH FEDERAL REGULATIONS RELATING TO RED FLAGS AND IDENTIFY THEFT; TO COMPLY WITH SOUTH CAROLINA ACT 190,THE FINANCIAL IDENTITY FRAUD AND IDENTITY THEFT PROTECTION ACT OF 2008; TO PROVIDE FOR CODIFICATION; TO PROVIDE FOR SEVERABILITY; TO PROVIDE FOR AN ADOPTION DATE; TO PROVIDE AN EFFECTIVE DATE; AND FOR OTHER PURPOSES ALLOWED BY LAW.

WHEREAS, the State of South Carolina has enacted the Financial Identity Fraud and Identity Theft Protection Act of 2008, also referred to as Act 190 of 2008;

WHEREAS, Article 3, Chapter 2, Title 30 of Act 190 specifically provides procedures for state and local governments to ensure the protection of personal identifying information belonging to members of the public that are in their possession;

WHEREAS, pursuant to federal law the Federal Trade Commission adopted Identity Theft Rules requiring the creation of certain policies relating to the use of consumer reports, address discrepancy and the detection, and prevention and mitigation of identity theft;

WHEREAS, the Federal Trade Commission regulations, codified at 16 CFR § 681.2 require creditors, as defined by 15 U.S.C. § 168a(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 Federal Trade Commission regulations include utility providers in the definition of a creditor;

WHEREAS, the Federal Trade Commission regulations includes non-utility accounts such as hospitals and emergency service providers as payment for these services are deferred;

WHEREAS, the Federal Trade Commission 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 Federal Trade Commission 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, customer accounts for *Fairfield County* EMS for which payment is made after the product is consumed or the service has otherwise been provided are covered accounts by virtue of being for household purposes and allowing for multiple payments or transactions;

WHEREAS, the Federal Trade Commission regulations, codified as 16 CFR 681.1, require users of consumer credit reports to develop policies and procedures relating to address discrepancies between information provided by a consumer and information provided by a consumer credit company;

NOW THEREORE, be it ordained that the County Of Fairfield adopts the following Identity Theft Prevention Program:

GENERAL PROVISIONS

The Code of the County of Fairfield is hereby amended by adding an Article to be numbered 547, which said Article reads as follows:

"Article 547

Identity Theft Prevention Program
Section __A__-1. Short Title.

This article shall be known as the Identity Theft Prevention Program.

Section __B__-2. Purpose.

The purpose of this Article is to comply with Act 190 of 2008 of the South Carolina Code of Laws, and 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 __C__-3. Definitions.

For purposes of this Article, the following definitions apply[1]:

---

[1] Other than "breach of security system", "county", "covered account", and "personal identifying information", definitions provided in this section are based on the definitions provided in 16 CFR § 681.2.

(a) 'Breach of the security system' as defined under SC Code of Laws §1-11-490 means unauthorized access to and acquisition of computerized data that was not rendered unusable through encryption, redaction, or other methods that compromise the security, confidentiality, or integrity of personal identifying information maintained by a county or county entity, when illegal use of the information has occurred or is reasonably likely to occur or use of the information creates a material risk of harm to the consumer. Good faith acquisition of personal identifying information by an employee or agent of the county or entity for the purposes of the county or entity is not a breach of the security of the system if the personal identifying information is not used or subject to further unauthorized disclosure.

(b) 'County' means the County of Fairfield.

(c) 'Covered account' means an account that Fairfield County offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions for which there is a reasonably foreseeable risk to customers or to the safety and soundness of account information from identity theft, including financial, operational, compliance, reputation, or litigation risks.

(d) '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.

(e) '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.

(f) 'Customer' means a person that has a covered account with a creditor.

(g) 'Identity theft' means a fraud committed or attempted using identifying information of another person without authority, and includes any terms and definitions as defined in SC Code of Laws §16-13-510.

(h) 'Notice of address discrepancy' means a notice sent to a user by a consumer reporting agency pursuant to 15 U.S.C. § 1681(c)(h)(1), that informs the user of a substantial difference between the address for the consumer that the user provided to request the consumer report and the address(es) in the agency's file for the consumer.[2]

---

[2] See 16 CFR § 681.1(b).

(i) 'Person' means a natural person, a corporation, government or governmental subdivision or agency, trust, estate, partnership, cooperative, or association.

(j) 'Personal Identifying Information' under the South Carolina Financial Identity Fraud and Identity Theft Protection Act (Act 190 of 2008) includes, but is not limited to: (1) social security numbers; (2) driver's license information; (3) checking and savings account numbers; (4)credit card numbers; (5) debit card numbers; (6) personal identification numbers; (7) electronic identification numbers; (8) digital signatures; (9) passports; (10) birth certificates; (11) immigration documents; (12) state issued identification cards; (13) other numbers or information which may be used to access a person's financial resources such as a password.

(k) 'Red flag' means a pattern, practice, or specific activity that indicates the existence of possible identity theft.

(l) 'Service provider' means a person that provides a service directly to the county.

Section __D__-4. Findings.

(1) The South Carolina General Assembly finds that the social security number and other personal identifying information can be used as tools to perpetuate fraud against an individual and to acquire sensitive personal, financial, medical, and familial information, the release of which could cause great financial or personal harm to the individual.

Section __E__-5. Personal Identifying Information Privacy Protection

(1) Although there are legitimate reasons for local government entities to collect social security numbers and other personal identifying information from individuals, [*County*] will collect the information only for legitimate purposes or when required by law.
(2) [*County*] that possess social security numbers or other personal identify information will use reasonable efforts to minimize instances of this information's dissemination either internally within government or externally with the general public.
(3) [*County*] will collect no more than five digits of an individual's social security number unless authorized by law to do so or unless the collection of the social security number is otherwise imperative for the performance of the [*county*]'s duties and responsibilities as prescribed by law.
(4) [*County*] shall segregate a social security number from the rest of the record, or as otherwise appropriate, so that the social security number may be easily redacted pursuant to a public records request.
(5) [*County*] will require an individual to transmit their social security number or other personal identifying information over the internet unless the connection is secure or the personal identifying information is encrypted.

(6) The [*county*] will remove or otherwise sanitize technology hardware such as computers that contain personal and confidential information before such hardware is disposed or transferred.
(7) The [*county*] shall dispose of its records that contain personal identifying information by modifying, shredding, erasing, or other means, so that the information is unreadable and undecipherable.

Section _F__-6. Outside Service Providers

In the event that the(name of county) county engages a service provider to perform an activity that involves the use of, or access to, personal identifying information that is in the county's possession, the (chief administrative officer or county personnel responsible for service contracts) shall exercise his or her discretion in reviewing such arrangements in order to ensure, to the best of his or her ability, that the service provider's activities are conducted in accordance with policies and procedures, agreed upon by contract, to ensure that the personal identifying information is treated in a confidential manner and that the service provider take appropriate steps to prevent or mitigate identity theft.

Section __G__-7. Security Breach

Fairfield County shall disclose a breach in the security data to a resident of this State whose unencrypted and unredacted personal identifying information was, or is reasonably believed to have been, acquired by an unauthorized person, when the illegal use of the information has occurred or is reasonably likely to occur or use of the information creates a material risk of harm to the resident. Disclosure shall be done in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement as provided in SC Code of Laws §1-11-490(C), or with measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. [*If the red flag rules compliance provisions below do not apply to your county, go directly to the "Ordinance Adoption" section*]

RED FLAG RULES COMPLIANCE PROVISIONS

Section __H__- . Process of Establishing a Covered Account.

For counties that provide service programs that fall under the federal red flag regulations, the following applies:

(1) As a precondition to opening a covered account in the county, each applicant shall provide the county with personal identifying information of the customer *[a valid SC driver's license or id card issued by SCDMV or, for customers who are not natural persons, a photograph of the customer's agent opening the account. If applicable to your county the following could also be included: "Such applicant shall also provide any information necessary for the department providing the service for which the covered account is created to access the*

applicant' s consumer credit report".] Such information shall be entered directly into the county's computer system and shall not otherwise be recorded.

(2) Each account shall be assigned an account number and personal identification number (PIN) which shall be unique to that account. The county may utilize computer software to randomly generate assigned PINs and to encrypt account numbers and PINs.[*If the county or county entity does not allow online payments, a PIN number may not be necessary*]

Section __I__- . Access to Covered Account Information.

(1) Access to customer accounts shall be password protected and shall be limited to authorized county personnel.
(2) Such password(s) shall be changed by *[the director of the department]* on a regular basis, shall be at least 8 characters in length and shall contain letters, numbers and symbols.
(3) Any unauthorized access to or other breach of customer accounts is to be reported immediately to the Chief Administrative Officer of the County and the password changed immediately.
(4) Personal identifying information included in customer accounts is considered confidential and any request or demand for such information shall be immediately forwarded to the Chief Administrative Officer of the County and the County Attorney.

Section __J__– . Credit Card Payments.

(1) In the event that credit card payments that are made over the internet are processed through a third party service provider, such third party service provider shall certify that it has an adequate identity theft prevention program in place that is applicable to such payments.
(2) All credit card payments made over the telephone or the county's website shall be entered directly into the customer's account information in the computer data base.
(3)Payments made on the website shall be made on a secured server.
(4) Account statements and receipts for covered accounts shall include only the last four[*note that state and federal law allows you to show up to five digits, although in practice, most merchants only show the last four digits*]digits of the credit or debit card or the bank account used for payment of the covered account.

Section __K__- . 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 and such red flags may include:

(1) Alerts from consumer reporting agencies, fraud detection agencies or service providers. Examples of alerts include but are not limited to:

a. A fraud or active duty alert that is included with a consumer report;
b. A notice of credit freeze in response to a request for a consumer report;
c. A notice of address discrepancy provided by a consumer reporting agency;
d. Indications of a pattern of activity in a consumer report that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:
    i. A recent and significant increase in the volume of inquiries;
    ii. An unusual number of recently established credit relationships;
    iii. A material change in the use of credit, especially with respect to recently established credit relationships; or
    iv. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

(2) *Fairfield County debt set off program*, a notice from the South Carolina Department of Revenue that there is no match between the name and social security number submitted for tax return garnishment.

(3) Suspicious documents. Examples of suspicious documents include:

e. Documents provided for identification that appear to be altered or forged;
f. Identification on which the photograph or physical description is inconsistent with the appearance of the applicant or customer;
g. Identification on which the information is inconsistent with information provided by the applicant or customer;
h. Identification on which the information is inconsistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check; or
i. An application that appears to have been altered or forged, or appears to have been destroyed and reassembled.

(4) Suspicious personal identification, such as suspicious address change. Examples of suspicious identifying information include:

j. Personal identifying information that is inconsistent with external information sources used by the financial institution or creditor. For example:
    i. The address does not match any address in the consumer report; or
    ii. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.
k. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer, such as a lack of correlation between the SSN range and date of birth.
l. Personal identifying information or a phone number or address, is associated with known fraudulent applications or activities as indicated by internal or third-party sources used by the financial institution or creditor.
m. 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.

n. The SSN provided is the same as that submitted by other applicants or customers.
o. 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.
p. 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.
q. Personal identifying information is not consistent with personal identifying information that is on file with the financial institution or creditor.
r. The applicant or customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

(5) Unusual use of or suspicious activity relating to a covered account. Examples of suspicious activity include:

s. Shortly following the notice of a change of an address for an account, county receives a request for the addition of authorized users on the account.
t. A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example:
    i. The customer fails to make the first payment or makes an initial payment but no subsequent payments.
u. An account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:
    i. Nonpayment when there is no history of late or missed payments;
    ii. A material change in purchasing or spending patterns;
v. An account that has been inactive for a long period of time is used *(taking into consideration the type of account, the expected pattern of usage and other relevant factors)*.
w. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's account.
x. The county is notified that the customer is not receiving paper account statements.
y. The county is notified of unauthorized charges or transactions in connection with a customer's account.
z. The county is notified by a customer, law enforcement, state, federal, or local government entity, or other person that it has opened a fraudulent account for a person engaged in identity theft.

(6) Notice from customers, law enforcement, victims or other reliable sources regarding possible identity theft or phishing (an attempt at fraud based on the theft of the identity of a trusted person or organization, for the purpose of stealing personal information, usually in the form of an e-mail or website claiming to be legitimate seeking identifiable information) relating to covered accounts

Section _ L___- . Prevention and Mitigation of Identity Theft.

(1) In the event that any county 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 or her

discretion to determine whether such red flag or combination of red flags suggests a threat of identity theft. If, in his or her discretion, such employee determines that identity theft or attempted identity theft is likely or probable, such employee shall immediately report such red flags to the Department Head. If, in his or her discretion, such employee deems that identity theft is unlikely or that reliable information is available to reconcile red flags, the employee shall convey this information to County Administrator or Deputy, who may in his or her discretion determine that no further action is necessary. If the County Administrator or Deputy in his or her discretion determines that further action is necessary, a county employee shall perform one or more of the following responses, as determined to be appropriate by Administration:

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. Cease attempts to collect additional charges from the customer and decline to sell the customer's account to a debt collector in the event that the customer's account has been accessed without authorization and such access has caused additional charges to accrue;
d. Notify a debt collector within *, 24 hours* of a discovery of likely or probably identity theft relating to a customer account that has been sold to such debt collector in the event that a customer's account has been sold to a debt collector prior to the discovery of the likelihood or probability of identity theft relating to such account;
e. Notify law enforcement, in the event that someone other than the customer has accessed the customer's account causing additional charges to accrue or accessing personal identifying information; or
f. Take other appropriate action to prevent or mitigate identity theft.

(2) In the event that any county employee responsible for, or involved in, opening a new covered account becomes aware of red flags indicating possible identity theft with respect an application for a new account, such employee shall use his or her discretion to determine whether such red flag or combination of red flags suggests a threat of identity theft. If, in his or her discretion, such employee determines that identity theft or attempted identity theft is likely or probable, such employee shall immediately report such red flags to the Department Head. If, in his or her discretion, such employee deems that identity theft is unlikely or that reliable information is available to reconcile red flags, the employee shall convey this information to County Administrator or Deputy, who may in his or her discretion determine that no further action is necessary. If the County Administrator or Deputy in his or her discretion determines that further action is necessary, a county employee shall perform one or more of the following responses, as determined to be appropriate by Administration:

a. Request additional identifying information from the applicant;
b. Deny the application for the new account;
c. Notify law enforcement of possible identity theft; or
d. Take other appropriate action to prevent or mitigate identity theft.

Section __M__- . Updating the Program.

The FAIRFIELD COUNTY COUNCIL shall annually review and, as deemed necessary by the COUNTY COUNCIL, update 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 county and its covered accounts from identity theft. In so doing, the FAIRFIELD COUNTY COUNCIL shall consider the following factors and exercise its discretion in amending the program:

(1)The county's experiences with identity theft;
(2)Updates in methods of identity theft;
(3)Updates in customary methods used to detect, prevent, and mitigate identity theft;
(4)Updates in the types of accounts that the county offers or maintains;
(5)Updates in service provider arrangements.

Section _N__- . Program Administration.

Deputy County Administrator is responsible for oversight of the program and for program implementation. The County Administrator is responsible for reviewing reports prepared by staff regarding compliance with red flag requirements and with recommending material changes to the program, as necessary in the opinion of the *Cou*nty Administrator, to address changing identity theft risks and to identify new or discontinued covered types of covered accounts. Any recommended material changes to the program shall be submitted to the FAIRFIELD COUNTY COUNCIL for consideration by the FAIRFIELD COUNTY COUNCIL.

(1)The *Deputy County Administrator* will report to the County Administrator at least annually, on compliance with the red flag requirements. The report will address material matters related to the program and evaluate issues such as:

a. The effectiveness of the policies and procedures of county in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts;
b. Service provider arrangements;
c. Significant incidents involving identity theft and management's response; and
d. Recommendations for material changes to the Program.

(2)The *Deputy County Administrator* is responsible for providing training 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 with respect to the implementation and requirements of the Identity Theft prevention Program. The *Deputy County Administrator* shall exercise his or her discretion in determining the amount and substance of training necessary.

Section __O__- . Outside Service Providers.

In the event that the county engages a service provider to perform an activity in connection with one or more covered accounts the Purchasing Director and County Attorney shall exercise his or her discretion in reviewing such arrangements in order to ensure, to the best of his or her ability, that the service provider's activities are conducted in accordance with policies and procedures, agreed

upon by contract, that 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.

Section __P__- . Methods of confirming Consumer Addresses.

The county employee charged with confirming consumer addresses may, in his or her discretion, confirm the accuracy of an address through one or more of the following methods:

(1)Verifying the address with the consumer;
(2)Reviewing the county's records to verify the consumer's address;
(3)Verifying the address through third party sources; or
(4)Using other reasonable processes.

ORDINANCE ADOPTION

[*The following unnumbered sections are incorporated in any ordinance*]

Section A-P.

The preamble to this ordinance is hereby incorporated into this ordinance as if set out fully herein.

Section A-P.

All ordinances and parts of ordinances in conflict herewith are hereby expressly repealed.

Section A-P.

The adoption date of this ordinance is June 8, 2009.

Section ____-.

The effective date of this ordinance is June 8, 2009.

ORDAINED by the County Council of Fairfield this the 8th day of June, 2009.

ATTEST:

By Sheryl K Brown
Clerk to the Council

Chairman Russell Real Brown

County of Fairfield