ACCG
Identity Theft Prevention Program

ACCG
50 Hurt Plaza, Suite 1000
Atlanta, Georgia 30303
(404)522-5022
(404)525-2477
www.accg.org

June 2010

Contents

Summary of ACCG Identity Theft Prevention Program

The Federal Trade Commission (FTC) will begin enforcement of its "Red Flags Rules," a result of the Fair and Accurate Credit Transactions Act of 2003 (FACTA), on January 1, 2011. The penalty for noncompliance with the Red Flags Rule is up to $3,500 per violation. This federal law was enacted to require financial institutions and "creditors" with "covered accounts" to implement a program to detect, prevent and mitigate instances of identity theft. However, the interpretation of "creditor" is fairly broad and may include several Georgia counties.

Because many counties provide ambulance services or emergency transport where the cost is billed to the patient after the transport, they are considered a "creditor" with a "covered account." See, 16 U.S.C. § 681.2(b)(3). Although this policy mostly focuses on ambulance/EMS service, FACTA will also apply to other services for which the County bills after the service is provided. Utility service is an example. Under this federal law, the County is required to have a written identity theft prevention program to detect, prevent and mitigate identity theft of patient account information.

Below are the steps that the County must take to comply with FACTA:

1. Make sure that the County's Health Insurance Portability and Accountability Act ("HIPAA") compliance program is up to date, if the County is a "covered entity." If your county is providing EMS/ambulance transport to citizens for a fee, then the County is likely to be a "covered entity" under HIPAA. The County's HIPAA compliance program will likely help the County to comply with the requirements of FACTA. It may make sense to just add references to the Identity Theft Prevention Program.

2. Identify which accounts are "covered accounts" under FACTA. See, 16 C.F.R. § 681.2(c). A "covered account" is (1) an account primarily for personal, family or household purposes that involves or is designed to permit multiple payments or transactions; or (2) any other account for which there is a reasonably foreseeable risk to customers or the safety and soundness of the [county] from identity theft. 16 C.F.R. § 681.2(b)(3).

3. Perform a risk assessment on the "covered accounts." This risk assessment is to see which accounts have a high risk of identity theft. The County must consider: (1) the way that it opens accounts; (2) the way that it provides/allows access to the accounts; and (3) past experience with identity theft. 16 C.F.R. § 681.2(c)(1)-(3).

4. Develop and implement a written identity theft prevention program to address identity theft risks referred to as "red flags." A "red flag" is a pattern, practice or specific activity that indicates the possible existence of identity theft. 16 C.F.R. § 681.2(b)(9). In other words, suspicious activity that raises a "red flag." The written identity theft prevention program must include policies and procedures to: (1) identity relevant red flags; (2) detect red flags; (3) explain appropriate responses for when a red flag is discovered; and (4) address how the program is updated to reflect the changes in risk to patients (or customers) and to reflect changes in the safety and soundness of the County from identity theft. 16 C.F.R. § 681.2(d)(2).

5. Administer the identity theft prevention program. The County must: (1) get official approval from the Board of Commissioners, Sole Commissioner or Council; (2) ensure that a senior level of County management will oversee the development, implementation and administration of the program; (3) train staff;

and (4) make sure that parties who contract with the County for services related to the accounts sign business associate agreements or otherwise ensure compliance with FACTA. See, 16 C.F.R. § 681.2(2) and 16 C.F.R. § 681.2(e).

Attached is a Sample Resolution to Adopt Identity Theft Prevention Program, as well as a Sample Identity Theft Prevention Program. Counties should work closely with their County Attorney and staff who deal with these accounts to tailor this policy to fit the processes that the County uses. A sample letter that can be used to notify a patient (or customer) of a suspected identity theft is also included. The FTC has prepared an affidavit and compliant form that these patients (or customers) can use.

For more on how to comply with the Red Flags Rule, the FTC has prepared, "Fighting Fraud with the Red Flags Rule" to assist organizations in implementing a written Identity Theft Prevention Program designed to detect the warning signs of identity theft at www.ftc.gov.

-- June 2010

Sample Resolution to Adopt Identity Theft Prevention Program

Below is a resolution to adopt the Identity Theft Prevention Program. This should be adopted in an open meeting after the resolution and program have been carefully reviewed by the County Attorney and appropriate County staff to tailor the program to meet the County's needs.

_____ County
Board of Commissioners/Commissioner/Council Resolution
to Adopt an Identity Theft Prevention Program

WHEREAS, the federal government has found identity theft is a serious problem for "creditors" (i.e., providers of services when the fee for the service is collected after the service is provided) in the United States;

WHEREAS, the federal government has determined that counties that provide emergency medical service ("EMS"), ambulance service [*and other services or utilities if the county provides services in exchange for payment after the service is rendered]* may be considered "creditors";

WHEREAS, in response to the risks posed by identity theft to consumers, the United States Congress enacted the Fair and Accurate Credit Transactions Act of 2003 ("FACTA");

WHEREAS, the Federal Trade Commission ("FTC"), along with federal bank regulators, adopted regulations implementing the FACTA (the "Red Flag Rules") that require creditors to adopt a written Identity Theft Prevention Program.

WHEREAS, because _____ County provides EMS, ambulance service *[and any service provided by the County where the user pays after the service is delivered]*, the Board of Commissioners/Commissioner/Council believes that it is a creditor subject to the FTC's Red Flag Rules; and

WHEREAS, in order to comply with FACTA and the Red Flag Rules, _____ County has developed a written Identity Theft Prevention Program designed to detect, prevent, and mitigate identity theft.

NOW THEREFORE BE IT RESOLVED by the Board of Commissioners/Commissioner/Council that the attached Identity Theft Prevention Program is adopted and *[Insert Title of County Employee Who Will be in Charge of Red Flag Rules Compliance]* is appointed as Red Flags Compliance Officer and is delegated responsibility for oversight, ongoing development, implementation, and administration of the program and shall have the responsibility to develop periodic updates to the program to reflect changes in risk to customers and to the safety and soundness of _____ County.

This _____ day of _____, 20____.

The _____ County Board of Commissioners/Commissioner/Council

Sample Identity Theft Prevention Program

This program should be reviewed and redrafted by the County Attorney and the County staff who regularly deal with patient accounts to tailor it appropriately to the accounts and processes employed by the County.

_____ County
Identity Theft Prevention Program

Purpose

This policy sets forth _____ County's commitment to comply with the standards established by the Federal Trade Commission under the Identity Theft Red Flags and Address Discrepancies under the Fair and Accurate Credit Transaction Act of 2003 ("the Red Flag Rules"). 16 C.F.R. § 681.2. This Identity Theft Prevention Program ("Program") is designed to detect, prevent and mitigate identity theft in connection with the opening of a "covered account" (i.e., ambulance patients' accounts *[or, if the County provides utility services, "customer accounts"]*) or any existing "covered account."

Scope

This Program contains policies and procedures that are designed to identify, detect and respond to suspicious activity on ambulance patient's billing accounts *[and any utility accounts that the County may maintains]* of _____ County. This Program will provide County staff the direction to respond appropriately to "Red Flags" or suspicious activity that indicate the possibility of identity theft on these accounts. It also contains policies and procedures for the periodic identification of "covered accounts" and for the general administration of the Program. As a "creditor" with "covered accounts" under the Red Flag Rules, _____ County is required to:

1. Periodically identify "covered accounts";

2. Establish a written Identity Theft Prevention Program; and

3. Administer the Identity Theft Prevention Program.

Definitions

(a) "Covered account" means:

1. An account that _____ County offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions; and

2. Any other account that _____ County offers or maintains for which there is a reasonably foreseeable risk to individuals or to the safety and soundness of _____ County from identity theft, including financial, operational, compliance, reputation, or litigation risks.

This includes patient ambulance accounts *[if the County offers any other services for which it bills after the service is provided, such as a utility, these services should be identified and added her].*

(b) "Identity theft" means a fraud committed or attempted using the identifying information of another person without authority.

(c) "Identifying information" means a person's name, credit card account information, debit card information, bank information, drivers' license information, social security number, government issued identification number, alien registration number, government issued passport number, employer or taxpayer identification number, mother's birth name, date of birth, health insurance information, Medicare or Medicaid number and/or health care claim number.

(d) "Program" means this written Identity Theft Prevention Program developed and implemented by _____ County.

(e) "Red Flag" means a pattern, practice, or specific or suspicious activity that indicates the possible existence of identity theft.

(f) "Red Flags Compliance Officer" means that person appointed by the Board of Commissioners/Commissioner/Council who has the responsibility for oversight, ongoing development, implementation, and administration of the Program and who has the responsibility to develop periodic updates to the program to reflect changes in risk to customers and to the safety and soundness of the organization.

(g) "Service provider" means a person or company that provides a service directly to _____ County, including third party billing companies and other organizations that perform service in connection with _____ County's covered accounts.

Procedure: Identify Covered Accounts

(a) Each year, the Red Flags Compliance Officer shall make a recommendation to the Board of Commissioners/Commissioner/Council as to whether the County continues to offer or maintain covered accounts (see definition of "covered account" in this Program). The Red Flags Compliance Officer shall document this determination.

(b) Each year, the Red Flags Compliance Officer shall conduct an annual risk assessment of the County's accounts to determine whether it offers or maintains accounts that carry a reasonably foreseeable risk to patients [*if the County provides other services that are covered, add "customers" or*

other word to describe those who receive the service] or to the safety and soundness of _____ County from identity theft, including financial, operational, compliance, reputation, or litigation risks. In determining whether _____ County offers or maintains such accounts, the Red Flags Compliance Officer will conduct an annual risk assessment that takes into consideration:

1. The methods that the County uses to open its accounts;

2. The methods that the County uses to access its accounts; and

3. The County's previous experiences with identity theft, if any.

(c) When possible, the annual identification of covered accounts will be conducted by an evaluation or audit team appointed by and acting under the direction and control of the Board/Commissioner/Council.

Procedure: Identify Red Flags

(a) Once the Red Flags Compliance Officer has identified the County's covered accounts, he or she shall identify Red Flags (see definition in this Program) for those accounts. This shall be conducted on an annual basis in conjunction with _____ County's identification of covered accounts. The Red Flags Compliance Officer will also identify red flags as they arise and incorporate them into this Program.

(b) The Red Flags Compliance Officer shall consider the following factors in identifying relevant Red Flags for covered accounts, as appropriate:

1. The types of covered accounts that the County offers or maintains;

2. The methods that the County provides to open its covered accounts;

3. The methods that the County provides to access its covered accounts; and

4. Any incidents of identity theft that _____ County has experienced.

(c) The Red Flags Compliance Officer shall also consider the examples of Red Flags listed in Supplement A to Appendix A to 16 C.F.R. Part 681. The Program shall include relevant Red Flags from the following categories, as appropriate:

1. Alerts, notifications and other warnings from consumer report agencies or service providers, such as fraud detection services;

2. The presentation of suspicious documents;

3. The presentation of suspicious personal identifying information, such as a suspicious address change;

4. The unusual use of an address change;

5. Notice from customers, victims of identity theft, law enforcement or other persons regarding possible identity theft in connection with covered accounts.

(d) The Red Flags Compliance Officer shall also incorporate Red Flags from sources such as:

1. New and changing risks that he or she has identified; and

2. Any applicable supervisory guidance from the FTC or other appropriate sources.

(e) The following are Red Flags identified for _____ County's covered accounts as of the most recent update to this Program:

1. Patterns of activity on payment accounts that are inconsistent with prior history;

2. Increases in the volume of inquiries to an account;

3. The presentation of information that is inconsistent with other sources, (e.g., the address, date of birth, or social security number listed for the patient does not match the address given or is inconsistent with other identifying information provided by the patient *[or customer, if County provides utility or other services*]*)*;

4. Personal identifying information is identified by third-party sources as having been associated with known fraudulent activity;

5. Personal identifying information is of a type commonly associated with fraudulent activity (e.g., fictitious address, use of mail drop, or phone number that is invalid or associated only with a pager or answering service);

6. The social security number provided by the patient [*or customer, if County provides utility or other services]* is a duplicate of that of other patients;

7. The address or telephone numbers given are the same or similar to those of other patients *[or customer, if County provides utility or other services]*, particularly recent ones;

8. Attempts to access an account by persons who cannot provide authenticating information;

9. Requests for additional authorized users on an account shortly following change of address;

10. Uses of an account that are inconsistent with established patterns of activity (e.g., nonpayment when there is no history of late or missed payments);

11. Nonpayment of the first payment on the account;

12. Inactivity on an account for a reasonably lengthy period of time;

13. Mail correspondence sent to the provided address is returned and mail

is returned despite continued activity in the account;

14. Notification of an unauthorized transaction by the patient *[or customer, if County provides utility or other services]*;

15. Notification by the patient [*or customer, if County provides utility or other services]*, a law enforcement authority or other person that it has opened a fraudulent account;

16. A complaint or question from a patient *[or customer, if County provides utility or other services]* based on the patient's *[or customer's, if County provides utility or other services]* receipt of:

    a) A bill for another individual;

    b) A bill for a service that the patient *[or customer, if County provides utility or other services]* denies receiving;

    c) A bill from a health care provider that the patient never utilized;

    d) A notice of insurance benefits or Explanation of Benefits for health services never received; or

    e) A patient or insurance company report that coverage for legitimate healthcare service is denied because insurance benefits have been depleted or a lifetime cap has been reached.

17. A complaint or question from a patient about information added to a credit report by a health care provider or insurer;

18. A dispute of a bill by a patient *[or customer, if County provides utility or other services]* who claims to be the victim of any type of identity theft;

19. A patient who has an insurance number but never produces an insurance card or other physical documentation of insurance;

20. A notice or inquiry from an insurance fraud investigator for a private

insurance company or a law enforcement agency;

21. A security breach;

22. Unauthorized access to a covered account by personnel;

23. Unauthorized downloading of patient *[or customer, if County provides utility or other services]* files;

24. Loss or theft of unencrypted data;

25. Inappropriate access of a covered account;

26. A computer virus or suspicious computer program;

27. Multiple failed log-in attempts on a workstation;

28. Theft of a password;

29. The presentation of an insurance card or form of identification that is clearly altered; and

30. Lost, stolen or tampered County equipment.

Procedure: Detect Red Flags

(a) _____ County shall adopt reasonable policies and procedures to address the detection of Red Flags in connection with the opening of covered accounts and existing covered accounts by:

1. Obtaining identifying information about, and verifying the identity of, a person opening a covered account; and

2. Authenticating patients, monitoring transactions, and verifying the validity of change of address requests.

(b) The following procedures have been adopted by _____ County to address the detection of Red Flags as of the most recent update to this Program:

1. Suspicious Documents at the Time of Transport. _____ County personnel shall be on the alert for patients who present suspicious documents such as an insurance card or form of identification that appears to have been altered or does not match other information about the patient. Whenever possible, the crew shall attempt to verify the identity of the patient with someone who knows the patient and/or someone who has rendered care to the patient. **Personnel shall not delay the provision of care when verifying this information and should obtain this information after the transport when it could delay the provision of care.**

2. ID Verification before Discussing Patient Account Information or Change of Address. Before discussing any information related to a covered account with any individual, or making a change to address information in a covered account; _____ County personnel shall sufficiently ascertain the identity of the individual.

    a) If a patient *[or customer, if County provides utility or other services]* or appropriate representative makes a telephone inquiry or request regarding a patient *[or customer, if County provides utility or other services]* account, _____ County personnel shall

require the patient *[or customer, if County provides utility or other services]* or appropriate representative of the patient to verify the date of birth, social security number (or at least the last 4 digits), and address of the patient *[or customer, if County provides utility or other services]* to whom the account pertains.

b) If the patient *[or customer, if County provides utility or other services]* or appropriate representative of the patient presents in person to the Finance Department of _____ County, s/he shall be required to provide a valid government issued photo ID in addition to the date of birth, social security number (or last 4 digits), and address of the patient *[or customer, if County provides utility or other services]* to whom the account pertains.

c) If the patient *[or customer, if County provides utility or other services]* or appropriate representative of the patient is unable to provide the necessary information to verify the identity of the patient *[or customer, if County provides utility or other services]*, _____ County staff shall make a notation of the inquiry or address change request in the patient *[or customer, if County provides utility or other services]* account file and alert an appropriate supervisor without providing access or honoring the address change request.

3. Under the HIPAA Privacy and Security Rules, _____ County is required to implement policies and procedures regarding the protection of protected health information and to implement administrative, physical and technical safeguards to protect electronic protected health information. The following policies and procedures from _____ County's HIPAA compliance program serve the dual purpose of detecting identity theft in connection with the opening of and existing covered accounts at _____ County and they are hereby incorporated in this Program by reference:

[List any applicable HIPAA policies adopted by the County that would serve to detect identity theft in connection with the County's covered accounts.]

Procedure: Respond to Red Flags

(a) _____ County will respond to Red Flags of which it becomes aware in a manner commensurate with the degree of risk posed by the Red Flag. In determining an appropriate response, _____ County will consider aggravating factors that may heighten the risk of identity theft. For example, notice to _____ County that a patient *[or customer, if County provides utility or other services]* has provided information to someone fraudulently claiming to represent _____ County may suggest that identity theft is more likely.

(b) _____ County shall assess whether the Red Flag detected poses a reasonably foreseeable risk of identity theft and if it does, respond appropriately. If _____ County determines that the Red Flag does not pose a reasonably foreseeable risk of identity theft, it shall have a reasonable basis choosing not to respond to the Red Flag.

(c) If any personnel at _____ County believe identity theft has occurred or may be occurring, s/he shall immediately notify a supervisor. The supervisor will contact the designated Red Flag Rule Compliance Officer who will determine the appropriate response.

(d) Appropriate responses may include the following:

1. Monitoring a covered account for evidence of identity theft;

2. Contacting the patient [*or customer, if County provides utility or other services]*;

3. Changing any passwords, security codes, or other security devices that permit access to a covered account;

4. Reopening a covered account with a new account number;

5. Not opening a new covered account;

6. Closing an existing covered account;

7. Not attempting to collect on a covered account or not selling a covered account to a debt collector;

8. Notifying law enforcement; or

9. Determining that no response is warranted under the particular circumstances.

(e) Patient *[or Customer, if County provides utility or other services]* Notification. If there is a confirmed incident of identity theft or attempted identity theft, _____ County will notify the patient *(or customer, if County provides utility or other services)* after consultation with law enforcement about the timing and the content of such notification (to ensure notification does not impede a law enforcement investigation) via certified mail. Victims of identity theft will be encouraged to cooperate with law enforcement in identifying and prosecuting the suspected identity thief, and will be encouraged to complete the FTC Identity Theft Affidavit.

(f) Investigation of Suspected Identity Theft. If an individual claims to be a victim of identity theft, _____ County will investigate the claim. The following guidelines apply:

1. The individual will be instructed to file a report with law enforcement for identity theft.

2. The individual will be instructed to complete the FTC ID Theft Affidavit, including supporting documentation.

3. The individual will be requested to cooperate with comparing his or her personal information with information in _____ County's records.

4. If following investigation, it appears that the individual has been a victim of identity theft, _____ County will take the

following actions:

a) Cease collection on open accounts that resulted from identity theft. If the accounts had been referred to collection agencies or attorneys, the collection agencies/attorneys will be instructed to cease collection activity.

b) Cooperate with any law enforcement investigation relating to the identity theft.

c) If an insurance company, government program or other payor has made payment on the account, the provider will notify the payor and seek instructions to refund the amount paid.

d) If an adverse report had been made to a consumer reporting agency, the provider will notify the agency that the account was not the responsibility of the individual.

5. If following investigation, it does not appear that the individual has been a victim of identity theft, _____ County or the collection agency will give written notice to the individual that he or she is responsible for payment of the bill. The notice will state the basis for determining that the person claiming to be a victim of identity theft was in fact the patient *[or customer, if County provides utility or other services]*.

(g) Amendment of Records. Patient medical records and payment records must be corrected when identity theft has occurred. This is necessary to ensure that inaccurate health information is not inadvertently relied upon in treating a patient, and that a patient or a third-party payer is not billed for services the patient did not receive. Patient records will be corrected in consultation with the patient and the patient's treating health care provider(s), and in a manner consistent with the _____ County's HIPAA policy on amendments to medical records.

(h) Disclosure/Unauthorized Access to Unencrypted Data. If there is a disclosure of, or an unauthorized access to, unencrypted computerized

data containing a person's first name or first initial and last name and (1) a social security number, (2) driver's license number, or (3) financial account number (including a credit or debit card number), notify the patient *(or customer, if County provides utility or other services)*..

(i) The Presentation of Suspicious Documents at the Time of Transport._When a patient presents a suspicious document such as an insurance card or form of identification that is clearly altered or does not match other information about the patient, ambulance personnel shall:

1. Note the nature of the incident and circumstances surrounding the incident in an incident report or other appropriate document so that the claim is "flagged" for review.

2. If possible, attempt to obtain identifying information about the patient from other sources such as individuals who know or have treated the patient.

3. Notify the Red Flag Rules Compliance Officer as soon as possible after the transport about the incident and the circumstances surrounding the incident.

4. Before opening a covered account under the name given, the Red Flag Rules Compliance Officer, or other designated individual, shall make attempts to verify the identity of the patient though any means possible. If it appears the patient has attempted to commit identity theft, the procedures for notification and investigation of the incident (above) shall be followed.

Procedure: Update the Program

(a) _____ County shall update this Program (including identifying Red Flags determined to be relevant) annually.

(b) The update shall reflect changes in risks of identity theft to patients or to the safety and soundness of _____ County's information. The review and update will be based on factors such as:

1. The experiences of _____ County with identity theft;

2. Changes in methods of identity theft;

3. Changes in methods to detect, prevent, and mitigate identity theft;

4. Changes in the types of accounts that _____ County offers or maintains; and

5. Changes in the business arrangements of _____ County, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

Procedure: Administer the Program

(a) Program Oversight. The Board of Commissioners/Commissioner/Council has designated a Red Flag Rules Compliance Officer who is in charge of Red Flag Rules compliance. This individual shall be involved in the oversight, development, and implementation and administration of the Program. The individual shall be responsible for:

1. Implementation of this Program;

2. Reporting to the Board of Commissioners/Commissioner/Council, or an appropriate designated committee of the board at least annually on compliance by _____ County with this Program. The

report shall 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) Incidents involving identity theft and management's response; and

d) Recommendations for material changes to the Program.

(b) After reviewing official annual reports, the Board of Commissioners/Commissioner/Council or appropriate designated committee shall approve changes to this Identity Theft Prevention Program, as necessary.

Procedure: Train Employees

(a) _____ County will conduct a general training session for all personnel to provide them with a general overview of this Program. All new personnel shall undergo such training during their orientation process. Documentation of training, including copies of all rosters and sign in sheets showing the training dates and the names of attendees, shall be maintained for at least four years.

(b) All staff that are responsible for the administration of the Program and staff who regularly deal with covered accounts should be trained on an annual basis.

Procedure: Oversee Service Provider Arrangements

If _____ County engages a third party to perform an activity in connection with one or more covered accounts (*e.g*., billing companies, collection agencies), _____ County will:

(a) Review the third party's policies for preventing, detecting, and mitigating identity theft and determine if those policies are acceptable to _____ County; or

(b) Require the third party to comply with the applicable terms of this Program through contract or agreement.

Sample Letter to Notify Patient/Customer of Suspected Identity Theft

If the Red Flags Compliance Officer discovers or suspects that there has been an incident of identity theft, the following letter should be sent from the Red Flags Compliance Officer to the patient (or customer) whose identity was stolen. A copy of the FTC Identity Theft Complaint and Affidavit should be attached.

[Date]

Via Certified Mail, Return Receipt Requested
Article No. _____
[Patient or Customer Name and Address]

Re: Possible Identity Theft

Dear _____:

It appears that there may have been suspicious activity on your account maintained by _____ County on *[date]*. *[Explain the factual situation of the compromised information, how it happened, what information was disclosed and what actions have been taken to remedy the situation]*. This incident has been reported to the _____ County Sheriff's Office, which can be reached at _____. We have also placed an alert on your account in an effort to prevent further misuse of your identity.

Identity theft has become a serious problem that can cause financial harm. It may take a long time to correct. It is imperative that you take swift action. Medical identity theft can lead to inappropriate medical care when incorrect information is included in a patient's medical record. We request your assistance in ensuring that our records about you are correct.

If you find that you are a victim of identity theft, please take the following steps as soon as possible:

2. Fill out the attached FTC Identity Theft Complaint and Affidavit.
3. Contact the fraud departments of each of the three major credit bureaus and report the theft. Ask that a "fraud alert" be placed on your file and that

no new credit be granted without your approval. Below is the name and phone number of each of the major credit bureaus:

Equifax: 1.800.525.6285

Experian: 1.888.397.3742

Trans Union: 1.800.680.7289

4. For any accounts that have been fraudulently accessed or opened, contact the security department of the appropriate creditor or financial institution. You may want to consider closing these accounts. You should consider new passwords that are not your mother's maiden name or Social Security number on any new accounts you open.

5. Get a copy of the law enforcement report number or a copy of the report in case the bank, credit card company or others need proof of the crime later.

6. Call the Federal Trade Commission's ID Theft Clearinghouse toll-free at 1.877.ID.THEFT (1.877.438.4338) to report the theft. Counselors will take your complaint and advise you on how to deal with the credit-related problems that could result from ID theft. The Identity Theft Hotline and the ID Theft Website (www.ftc.gov/idtheft) give you one place to report the theft to the federal government and receive helpful information. By sharing your identity theft complaint with the FTC, you will provide important information that can help law enforcement officials track down identity thieves and stop them.

If it appears that you have been a victim of medical identity theft, then you should take the following steps:

1. Ask to review your medical records at the office of each of your medical provider's offices. If there is any incorrect information, you should advise the office of the appropriate corrections.

2. Carefully monitor explanations of benefits (EOBs) or other information that you receive from your health insurer to determine if any other person has used your identity to obtain health care. If you receive an EOB or medical

bill for a service that you did not receive, immediately contact your health insurance company and health care provider who furnished the services.

3. Notify other health care providers that your identifying information is being used in a fraudulent manner.

If there is anything that _____ County can do to assist you, please call me at _____.

Sincerely,

_____ County Red Flags Compliance Officer

Exhibit A

FTC Identity Theft Victims' Complaint and Affidavit