Charles County Government
Standard Operating Policy and Procedure

Title:	Identity Theft Prevention Program	**SOP #**:	CAD.1.013
Division:	ALL	**Effective Date**:	1/25/11
		Revision Date:	
		Page 1 of 14	
Purpose:	Charles County Government, Herein known as CCG is committed to providing all aspects of our service and conducting our business operations in compliance with all applicable laws and regulations. This policy sets forth our commitment to compliance with those 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") at 16 C.F.R. §681.2, regarding the establishment of a written Identity Theft Prevention Program ("Program") that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account.		
References:	Federal Trade Commission - Identity Theft Red Flags and Address Discrepancies under the Fair and Accurate Credit Transaction Act of 2003 ("the Red Flag Rules") at 16 C.F.R. §681.2 FTC Identity Theft Affidavit		
Policy:	This Program contains policies and procedures designed to identify, detect and respond appropriately to "Red Flags" for identity theft. It also contains policies and procedures for the periodic identification of covered accounts and for the general administration of the Program. This Program addresses our general approach to compliance with the Red Flag Rules. As a "creditor" with "covered accounts" under the Red Flag Rules, CCG is required to periodically identify covered accounts, establish a written Identity Theft Prevention Program and administer the Identity Theft Prevention Program.		

Procedure:	**Definitions** 1. "Account" means a continuing relationship established by a person with CCG to obtain services for personal, family, household or business purposes and includes an extension of credit, such as the purchase or services involving a deferred payment. 2. "Covered account" means: a. An account that CCG offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions; and b. Any other account that CCG offers or maintains for which there is a reasonably foreseeable risk to individuals of identity theft, including financial, operational, compliance, reputation, or litigation risks. 3. "Identity theft" means a fraud committed or attempted using the identifying information of another person without authority. 4. "Identifying information" means any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including any: a. Name, social security number, federal employer identification number, date of birth, official state or government issued driver's license or identification number, alien registration number, government passport number or employer or taxpayer identification number; b. Unique electronic identification number, address, or routing code; c. Telecommunication identifying information or access device (as those terms are defined in 18 U.S.C. §1029(e)); d. Customer account information; e. Credit card number; f. Bank account information; g. Medicare number; and

h. Health care claim number.

5. "Program" means this written Identity Theft Prevention Program developed and implemented by CCG.

6. "Red Flag" means a pattern, practice, or specific activity that indicates the possible occurrence of identity theft.

7. "Service provider" means a person who provides a service directly to CCG and includes third party billing companies and other organizations that perform service in connection with CCG's covered accounts.

Procedure

1. Identify Covered Accounts

    a. CCG will annually determine whether it offers or maintains covered accounts (see definition of "covered account" in this Program) and shall document that determination.

    b. As part of this annual identification of covered accounts, CCG shall conduct an annual risk assessment of its accounts to determine whether it offers or maintains accounts that carry a reasonably foreseeable risk of identity theft, including financial, operational, compliance, reputation, or litigation risks. During such annual risk assessment, CCG will take into consideration the following:

        I. The methods it uses to open its accounts;

        II. The methods it uses to access its accounts; and

        III. Its previous experiences with identity theft.

    c. The annual identification of covered accounts should be conducted by the Internal Auditor.

2. Identify Red Flags

    a. CCG shall consider the following factors in identifying relevant Red Flags for covered accounts:

        I. The types of covered accounts it offers or maintains;

        II. The methods it provides to open its covered accounts;

III. The methods it provides to access its covered accounts; and

IV. Any incidents of identity theft that CCG has experienced.

b. CCG shall consider relevant Red Flags from the following categories:

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

II. The presentation of suspicious documents;

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

IV. The unusual use of, or other suspicious address change;

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

c. CCG shall also incorporate Red Flags from sources such as:

I. New and changing risks that CCG has identified; and

II. Any applicable guidance from the Federal Trade Commission (FTC) or other appropriate sources.

d. The following are potential Red Flags activities identified for CCG's covered accounts as of the most recent update to this Program:

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

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

III. The presentation of information that is inconsistent with other sources, e.g., the address, date of birth, or social security number listed for the customer does not match the address given or is inconsistent with other identifying information provided by the customer;

IV. The presentation of credit card information or bank

	account information that does not belong to the customer; V. Credit card information or bank account information that is presented verbally or handwritten; VI. Personal identifying information is identified by third-party sources as having been associated with known fraudulent activity; VII. Personal identifying information 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); VIII. The social security number provided by a customer is a duplicate of another customer's; IX. The address or telephone numbers given are the same or similar to those of other customers, particularly recent ones; X. Attempts to access an account by persons who cannot provide authenticating information; XI. Requests for additional authorized users on an account shortly following change of address; XII. Uses of an account that are inconsistent with established patterns of activity such as: nonpayment when there is no history of late or missed payments; XIII. Nonpayment of the first payment on the account; XIV. Inactivity on an account for a reasonably lengthy period of time; XV. Mail correspondence sent to the provided address is returned and mail is returned despite continued activity in the account; XVI. Notification of CCG of an unauthorized transaction by the customer; XVII. Notification of CCG by the customer, a law enforcement authority, third party or other person, that the account was opened fraudulently;

XVIII. A complaint or question from a customer based on the customer's receipt of:

1. A bill for another individual;

2. A bill for a service that the customer denies receiving;

3. A bill from a health care provider that the customer never utilized;

4. A notice of insurance benefits (or Explanation of Benefits) for health services never received; or

5. Customer 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.

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

XX. A dispute of a bill by a customer who claims to be the victim of any type of identity theft;

XXI. A customer who has an insurance number but is unable to produce an insurance card or other physical documentation of insurance;

XXII. A notice or inquiry from an insurance fraud investigator for a private insurance company or a law enforcement agency;

XXIII. A security breach;

XXIV. Unauthorized access to a covered account;

XXV. Unauthorized downloading of customer files;

XXVI. Loss or theft of unencrypted data;

XXVII. Inappropriate access of a covered account;

XXVIII. A computer virus or suspicious computer program;

XXIX. Multiple failed log-in attempts on a workstation, or theft

of a password;

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

XXXI. Lost, stolen, or tampered facility equipment.

3. Detect Red Flags

a. CCG 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, such as by:

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

II. Authenticating customers, monitoring transactions, and verifying the validity of change of address requests.

b. The following procedures have been adopted by CCG to address the detection of Red Flags as of the most recent update to this Program:

I. Suspicious Documents at the Time of Service Delivery.
CCG personnel shall be on the alert if customers present documents such as an insurance card or other forms of identification that appears to have been altered or which do not match other identifying information about the customer. CCG personnel shall attempt to verify the identity of the customer with someone who knows the customer and/or someone who has previously provided services to that customer. CCG personnel shall not delay the provision of services when verifying this information and should obtain the information as soon as reasonably possible.

II. ID Verification Before Discussing Customer Account Information.
Before discussing any information related to a covered account with any individual, or making a change to address information in a covered account, CCG personnel shall sufficiently ascertain the identity of the individual.

1. If a customer or authorized representative makes a telephone inquiry or request regarding a customer account, CCG personnel shall require the customer or authorized representative of the customer to verify the date of birth, social security number (or at least the last 4 digits), and address of the customer to whom the account pertains.

2. If the customer or authorized representative of the customer presents in person to a business office of CCG, she/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 customer to whom the account pertains.

3. If the customer or authorized representative of the customer is unable to provide the required information to verify the identity of the customer, CCG staff shall make a notation of the inquiry or address change request in the customer account file and alert an appropriate supervisor without providing access or honoring the address change request until properly satisfied.

III. HIPAA Privacy and Security Rules.
CCG is required to implement policies and procedures regarding the protection of protected health information (PHI) and to implement administrative, physical and technical safeguards to protect electronic protected health information.

4. Respond to Red Flags

   a. CCG 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, CCG will consider aggravating factors that may heighten the risk of identity theft. For example, notice to CCG that a customer has provided information to someone fraudulently claiming to represent CCG may suggest that identity theft is more likely.

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

c. CCG personnel who believe identity theft has occurred or may be occurring, shall immediately notify the immediate supervisor. The supervisor will contact the designated Departmental Red Flag Rule compliance officer who will determine the appropriate response. (Each Department participating in this program shall designate a Red Flag Rule compliance officer for that Department.)

d. Appropriate responses may include the following:

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

II. Contacting the customer;

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

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

V. Not opening a new covered account;

VI. Closing an existing covered account;

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

VIII. Notifying law enforcement; or

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

e. Customer Notification.
If there is a confirmed incident of identity theft or attempted identity theft, the County Attorney's Office will notify the customer 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, the Department involved will investigate the claim. The following guidelines apply:

I. The individual will be instructed to file a police report for identity theft.

II. The individual will be instructed to complete the ID Theft Affidavit developed by the FTC, including supporting documentation; or an ID theft affidavit recognized under state law. (See attachment A.)

III. The individual will be requested to cooperate with comparing his or her personal information with information in CCG records.

IV. If following investigation, it appears that the individual has been a victim of identity theft, CCG will take the following actions:

1. 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.

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

3. 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.

4. 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.

V. If following investigation, it does not appear that the individual has been a victim of identity theft, CCG or the billing agency, if applicable, 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 customer.

g. Amendment of Records.
Customer account and payment records shall be corrected when identity theft has occurred to ensure that a customer or a third-party payer is not billed for services the customer did not receive. Customer account and payment records will be corrected in consultation with the customer.

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), state law governing notification of customers will be followed.

i. The Presentation of Suspicious Documents.
If a customer presents a suspicious document such as an insurance card or other form of identification that is clearly altered or does not match other information about the customer, CCG personnel shall:

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

II. If possible, attempt to obtain identifying information about the customer from other sources such as individuals who know or have provided services to the customer.

III. Notify the Departmental Red Flag Rules compliance officer as soon as possible after the occurrence by detailing the circumstances surrounding the incident.

IV. Before opening a covered account, the Departmental Red Flag Rules compliance officer, or other designated individual, shall make attempts to verify the identity of the customer through any means possible. If it appears the customer has attempted to commit identity theft, the procedures for notification and investigation of the incident shall be followed.

5. Update the Program

   a. Each participating Department shall update this Program (including identifying Red Flags determined to be relevant) if needed at the time an incident of identity theft or suspected identity theft occurs. The investigating Department shall analyze the current program's effectiveness and propose any changes to the County Administrator.

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

      I. The experiences of CCG with identity theft;

      II. Changes in methods of identity theft;

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

      IV. Changes in the types of accounts that CCG offers or maintains; and

      V. Changes in the business arrangements of CCG's, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

6. Administer the Program

   a. Program Oversight.
   Each Department participating in this program shall designate an individual who is in charge of Red Flag Rules compliance for that Department. This individual shall be involved in the oversight, development, and implementation and administration of the Program. The individual shall be responsible for:

      I. Implementation of this Program;

II. Reporting to their Department Head and to the County Administrator any incident of identity theft or suspected identity theft. The report shall address material matters related to the Program and evaluate issues such as:

1. The effectiveness of the policies and procedures of CCG in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts;

2. Service provider arrangements;

3. Incidents involving identity theft and management's response; and

4. Recommendations for material changes to the Program.

b. The County Administrator shall approve changes to this Identity Theft Prevention Program, as necessary.

7. Train Employees

a. Each Department participating in this program will conduct a general training session for their 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 is responsible for the administration of the Program and staff who regularly deal with covered accounts should be trained on an annual basis by their respective Department.

8. Oversee Service Provider Arrangements

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

	I. Review the third party's policies for preventing, detecting, and mitigating identity theft and determine if those policies are acceptable to CCG; or II. Require the third party to comply with the applicable terms of this Program through contract or agreement.	
Authorized:	Cindrei Lynn Kelly	Date: 1/26/11