

DHHS POLICY AND PROCEDURE MANUAL

Section VIII:	Privacy and Security
Title:	Identity Theft Red Flags and Address Discrepancy Policy
Chapter:	Identity Theft Policies
Current Effective Date:	09/1/09
Revision History:	
Original Effective Date:	09/1/09

Purpose

The purpose of the Identity Theft Red Flags and Address Discrepancy Policy is to require that divisions and offices within the North Carolina (NC) Department of Health and Human Services (DHHS) assess whether they must comply with the *Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003* (Red Flags and Address Discrepancy Rules). If compliance is necessary, then divisions and offices must develop and implement specific procedures to support the department's Identity Theft Prevention Program.

This policy is applicable to all DHHS divisions and offices.

Background

In response to the growing identity theft trends, industry regulators amended the Fair and Accurate Transactions Act of 2003 to include identity theft red flags and address discrepancy requirements. The Red Flags and Address Discrepancy Rules require financial institutions, creditors which own or maintain covered accounts, and debit or credit card issuers (debit/credit card issuers) to develop and implement the following program and/or procedures:

- An Identity Theft Prevention Program that enables either a *financial institution* or a *creditor* which *owns or maintains covered accounts* to detect, identify, and respond to patterns, practices, or specific activities that could indicate identity theft – known as “**red flags**”;
- Procedures that offer a *debit/credit card issuer* guidance in how to assess the validity of a change of address notification for a debit or credit card account and, within a short period of time afterwards, the card issuer receives a request for an additional or replacement card for the same account; and/or
- Procedures that detail how the *recipient of a credit report*, after receiving a notice of address discrepancy, should form a reasonable belief that a consumer's address has in fact changed, and provide the reasonably confirmed address to the consumer reporting agency from whom it received the notice of address discrepancy.

Section VIII:	Privacy and Security
Title:	Red Flag and Address Discrepancy Policy
Chapter:	Identity Theft Policies
Current Effective Date:	09/1/09

Initially, the mandatory compliance date for the Red Flags and the Address Discrepancy Rules was November 1, 2008. However, on October 22, 2008, the Federal Trade Commission (FTC) suspended Red Flag Rule enforcement until **May 1, 2009**, to give creditors and financial institutions additional time in which to develop and implement written identity theft prevention programs. On April 30, 2009, the FTC suspended enforcement a second time until **August 1, 2009**. On July 29, 2009, suspended enforcement again until **November 1, 2009** and further delay could be forthcoming. The compliance date for the Notice of Address Discrepancy Rule remains November 1, 2008.

Policy

DHHS is already committed to ensuring that its divisions and offices protect social security numbers (SSNs) and other identifying information of its clients from identity theft, in compliance with the department's **Identity Theft and Security Breach Notification Policy**. The Identity Theft Red Flags and Address Discrepancy Policy goes further to require that DHHS divisions and offices (divisions and offices) identify, prevent and mitigate any evidence of identity theft that arises in the course of their business.

The Red Flags and Address Discrepancy Rules apply broadly. Although one would not ordinarily think of divisions or offices operating as a financial institution, a creditor, or a debit/credit card issuer within the meaning of the Rules, divisions and offices do offer services and programs that can meet one or more of these categories. Accordingly, the Red Flags and Address Discrepancy Policy requires that DHHS establish a written *Identity Theft Prevention Program* and also develop and implement reasonable policies to respond to the notification of address changes, to the extent that a division or office issues debit/credit cards or utilizes consumer reports when extending credit.

In order for a division or office to officially determine whether it must comply with the Red Flags and Address Discrepancy Policy requirements, it must first assess whether it operates as a *financial institution, a creditor that offers or maintains covered accounts and/or a debit/credit card issuer*. If the division or office determines that it meets the definition of either of these three categories, it must perform a risk assessment and develop the required procedure(s).

Definitions

An **account** is a continuing relationship established by a person with a financial institution or creditor to obtain a product or service for personal, family, household or business purposes. Account includes: An extension of credit, such as during the purchase of property or services involving deferred payment.

A **cardholder** is a [client] who has been issued a debit or credit card.

The term **clear and conspicuous** means reasonably understandable and designed to call attention to the nature and significance of the information presented.

A **client** is an individual that receives services from programs offered by NC DHHS divisions and offices. For the purposes of this policy, a client can be considered a consumer who acquires services for direct use.

A **consumer reporting agency** is defined under the Fair Credit Reporting Act (FCRA) as any entity “which for monetary fees, dues or on a cooperative, non-profit basis regularly engages . . . in the practice of assembling or evaluating consumer credit information or other information on consumers.” It does not include governmental agencies or public law enforcement authorities. The extremely broad definition does include, however, private security firms hired by employers to conduct background checks and obtain information about employees and applicants. The Federal Trade Commission (the “FTC”), which enforces the FCRA, indicated in an opinion letter that this definition includes agencies retained by employers to investigate employees with respect to workers' compensation claims and other private entities and organizations hired by employers to investigate workplace misconduct such as sexual harassment allegations, fraud and employee violence. This expansive definition has not been confirmed in any court, as it is uncertain whether the FTC's broad interpretation will be adopted.

A **creditor** is any entity that regularly extends, renews, or continues credit; any entity that regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who is involved in the decision to extend, renew, or continue credit. Accepting credit cards as a form of payment does not in and of itself make an entity a creditor. Where non-profit and government entities accept deferred payment for goods or services, they, too, are to be considered creditors. Most creditors, except for those regulated by the Federal bank regulatory agencies and the National Credit Union Administration (NCUA), come under the jurisdiction of the Federal Trade Commission (FTC).

A **covered account is:** (i) 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 such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account; and (ii) 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.

A **financial institution** is defined as a state or national bank, a state or federal savings and loan association, a mutual savings bank, a state or federal credit union, or any other entity that, directly or indirectly, holds a “transaction account” belonging to a consumer. Most of these institutions are regulated by the Federal bank regulatory agencies and the NCUA. Financial institutions under the FTC's jurisdiction include state-chartered credit unions and certain other entities that hold consumer transaction accounts.

Identifying Information includes all of the items listed below. (N.C.G.S. § 14-113.20(b))

1. SSNs or employer identification numbers (EINs).

2. Drivers license, state identification card, or passport numbers.
3. Checking and savings account numbers.
4. Credit and debit card numbers.
5. Personal Identification Number (PIN) code, as defined in N.C.G.S. § 14-113.8(6).
6. Electronic identification numbers, electronic mail names or addresses, Internet account numbers, or Internet identification names.
7. Digital signatures.
8. Any other numbers or information that can be used to access a person's financial resources.
9. Biometric data.
10. Fingerprints.
11. Passwords.
12. Parent's legal surname prior to marriage.

Identity Theft is a fraud committed or attempted using the identifying information of another person without authority. (16 CFR 603.2(a))

Issue means to send out; put into circulation; or deliver for use.

A **notice of address discrepancy** is a notice sent to a user of a consumer report by a consumer reporting agency pursuant to 15 U.S.C. 1681c(h)(1), that informs the user of a substantial difference between the address for the consumer provided by the user in requesting the consumer report and the address or addresses the consumer reporting agency has in the consumer's file.

A **person** is any individual, partnership, corporation, trust, estate, cooperative, association, government or governmental subdivision or agency, or other entity.

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

A **service provider** is a person that provides a service directly to the financial institution, creditor, or debit/credit card issuer that deals with covered accounts.

A **transaction account** is a deposit or other account from which the owner makes payments or transfers. Transaction accounts include checking accounts, negotiable order of withdrawal accounts, savings deposits subject to automatic transfers, and share draft accounts.

Implementation

DHHS shall develop and implement an *Identity Theft Prevention Program*. As part of its program, divisions and offices shall assess whether they operate as a *financial institution*, a *creditor that offers or maintains covered accounts* and/or a *debit/credit card issuer*. If the division or office operates as either of these three, it is subject to this policy and must develop and implement the following procedure(s):

Financial Institution or a Creditor that owns or maintains covered accounts:

If the division or office determines that it operates as a financial institution or a creditor that owns or maintains covered accounts, the division or office must develop and implement reasonable procedures to detect, prevent and mitigate identity theft as part of the department's *Identity Theft Prevention Program*.

Debit/Credit Card Issuer:

If the division or office determines that it issues debit or credit cards, it must develop procedures to assess the validity of a request for a change of address that is followed closely by a request for an additional or replacement card. These procedures will be incorporated into the department's Identity Theft Prevention Program.

User of a Consumer Report:

If the division or office determines that it uses consumer reports as part of its business operations, it must develop procedures to respond to a notice of address discrepancy received from a consumer reporting agency. These procedures will be incorporated into the department's Identity Theft Prevention Program.

Department Responsibilities

The Red Flags Rule sets out how certain businesses and organizations must develop, implement, administer and oversee their Identity Theft Prevention Program. The Program must include four basic elements, which together create a framework to address the threat of identity theft.

Identity Theft Prevention Program Requirements

A. Basic Organizational Requirements

The purpose of the Identity Theft Prevention Program is to detect, prevent, and mitigate identity theft in connection with new or existing covered accounts. It must be appropriate to the **size**, **complexity**, **nature**, and **scope** of the department's activities.

B. Elements of the Program

First, the department's Program must include policies and procedures to identify the "red flags" of identity theft that a division or office may run across in the day-to-day operations of its business. For example, if a customer has to provide some form of identification to open an account, an ID that looks like it might be fake would be a "red flag" for a division or office.

Second, the Program must be designed to detect the red flags the division or office has identified. For example, if a division or office has identified fake IDs as a red flag, it must have procedures in place to detect possible fake, forged or altered identification.

Third, the Program must spell out appropriate actions the division or office will take when it detects red flags.

Fourth, because identity theft is an ever-changing threat, the division or office must address how it will re-evaluate its Program periodically to reflect new risks from this crime.

If a division or office issues debit and/or credit cards or uses consumer reports, the Program will also include procedures to:

- **Assess** the validity of a change of address for a debit or credit card account if an individual requests an additional or replacement card for the same account shortly thereafter; and/or
- **Enable** the recipient of a credit report, after receiving a notice of address discrepancy, to form a reasonable belief that a consumer's address has changed and to provide the reasonably confirmed address to the consumer reporting agency from whom it received the notice of address discrepancy.

C. *Administration of the Program*

DHHS provides for the continued administration of the *Identity Theft Prevention Program* by ensuring divisions and offices perform the following:

- **Obtaining** approval of the initial written Program from either the Secretary of DHHS (Secretary) or his or her designee;
- **Reporting to the Secretary** on exceptions, risks, and Program effectiveness;
- **Detecting, logging, and resolving** identified Red Flag exceptions;
- **Training management and staff** to effectively implement the divisions' and offices' procedures;
- **Exercising** effective oversight of Service Providers and binding them to compliance via contract;
- **Considering** the guidelines in Appendix B and **including** those guidelines that are appropriate in its procedures; and
- **Periodically monitoring** the divisions' and offices' procedures for changes in scope--which could include new covered accounts or red flags--legislation, and effectiveness.

D. *Oversight, Development, Implementation and Administration of the DHHS Identity Theft Program*

The Secretary of DHHS shall be responsible for designating an employee at the level of senior management to oversee the DHHS Identity Theft Program and assigning specific responsibility for the Program's implementation within the department.

Division or Office Responsibilities

In order for a division or office to determine whether the Red Flag and Address Discrepancy Policy applies to its business operations, the division or office shall perform a **risk assessment** (*See Appendix A*) by asking itself the following preliminary questions:

1. Is your division or office a creditor or financial institution?
2. If so, does your division or office offer or maintain covered accounts?
3. Does your division or office issue debit or credit cards?
4. Does your division or office order credit reports on consumers from a consumer reporting agency?
5. Is your division or office a service provider for another DHHS division or office that is subject to the Red Flag and/or Address Discrepancy Rules?
6. Is the service your division or office provides to the DHHS division or office covered by the Red Flag and/or Address Discrepancy Rules?

Those divisions and offices that are subject to the Red Flag and Address Discrepancy Rules will be required to perform the following functions as part of the DHHS Identity Theft Prevention Program:

- Identify their covered accounts;
- Identify their relevant red flags;
- Review/develop mechanisms to detect red flags;
- Review/develop mechanisms to prevent, mitigate, and respond to identity theft incidents;
- Add the Red Flag and Address Discrepancy Rules' requirements to their current identity theft compliance program activities;
- Ensure Service Providers' compliance with the Red Flag and Address Discrepancy Rules (covered accounts, transaction accounts, or debit/credit cards);
- Provide employee training; and
- Provide oversight of and review its procedures for effectiveness.

Guidelines for Formulating and Maintaining an Identity Theft Prevention Program

A. *Detecting Red Flags*

When the division or office performs a risk assessment and determines that it is subject to Red Flag Rule compliance, the division's or office's procedures should, at a minimum, address the detection of Red Flags in connection with the opening of covered accounts and with existing covered accounts, such as by:

- Obtaining identifying information about, and verifying the identity of, a person opening a covered account; and
- Authenticating customers, monitoring transactions, and verifying the validity of change of address requests, in the case of existing covered accounts.

The procedures should include relevant Red Flags from the following five categories, as appropriate (*See Appendix B for specific examples*):

- Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;
- The presentation of suspicious documents;
- The presentation of suspicious personal identifying information, such as a suspicious address change;
- The unusual use of, or other suspicious activity related to, a covered account; and
- Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the financial institution or creditor.

B. Preventing, Mitigating, and Responding to Identity Theft Incidents

The division's or office's procedures shall provide for appropriate responses to the red flags it has detected that are commensurate with the degree of risk posed. In determining an appropriate response, the division or office shall consider aggravating factors that may heighten the risk of identity theft, such as a data security incident that results in unauthorized access to a client's account records held by the division or office or third party, or notice that a client has provided information related to a covered account held by the division or office to someone fraudulently claiming to represent the division or office or to a fraudulent website. Appropriate responses may include the following:

- Monitoring a covered account for evidence of identity theft;
- Contacting the customer;
- Changing any passwords, security codes, or other security devices that permit access to a covered account;
- Reopening a covered account with a new account number;
- Not opening a new covered account;
- Closing an existing covered account;
- Not attempting to collect on a covered account or not selling a covered account to a debt collector;
- Notifying law enforcement; or
- Determining that no response is warranted under the particular circumstances.

NOTE: *In developing their policies and procedures for responding to red flags, DHHS divisions and offices must keep in mind that any responses they develop that involve the disclosure of health information or other confidential information must comply with the Health Insurance Portability and Accountability Act (HIPAA), the NC Identity Theft Protection Act, and state or federal substance abuse or mental health statutory or regulatory confidentiality provisions.*

C. Debit/Credit Card Issuers

A division or office that issues debit or credit cards must establish and implement reasonable policies and procedures to assess the validity of a change of address if it:

- Receives notification of a change of address for a consumer's debit or credit card account; and
- Within a short period of time afterwards (during at least the first 30 days), the division or office receives a request for an additional or replacement card for the same account.

Under these circumstances, the division or office is not allowed to issue an additional or replacement card, until:

- The cardholder is notified of the request:
 1. At the cardholder's former address; or
 2. By any other means of communication the division or office and the cardholder have previously agreed to use; and
- The cardholder is provided a reasonable means of promptly reporting incorrect address changes.

NOTE: *Any written or electronic notice that the division or office provides to the cardholder must be **clear and conspicuous** and provided separately from its regular correspondence with the cardholder.*

D. Oversight of Service Providers

Third-party service providers and business partners that handle information in covered, transaction, or debit/credit card accounts are probably one of the biggest risks related to identity theft. It is important for divisions and offices to be aware of how important this component is to the department's overall Identity Theft Prevention Program.

Whenever a division or office engages a service provider *outside of DHHS* to perform an activity in connection with one or more covered, transaction, or debit/credit card accounts on its behalf, the division or office shall take the necessary steps to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. The division or office shall require the service provider, **by contract** to do the following:

- Develop procedures to detect relevant Red Flags that may arise in the performance of its activities;
- Take appropriate steps to prevent identity theft;

- Mitigate identity theft immediately once it occurs; and
- Report all Red Flag incidents to the division or office within a specified time.

For example: The Office of the Controller (OC) contracts with the Attorney General’s Office to collect outstanding client debt on its behalf.

Whenever a division or office is a service provider that performs an activity for another division or office that is subject to the Red Flag and Address Discrepancy Rules, the service provider will also be required to develop policies and procedures.

For example: The Office of the Controller performs billing functions for Central Regional Psychiatric Hospital. As part of its billing functions, OC offers or maintains covered accounts on behalf of Central Regional Hospital. OC and Central Regional Hospital will be required to develop written procedures as part of the department’s Identity Theft Prevention Program.

E. Recording and Reporting Incidents

The Identity Theft and Security Breach Notification Policy requires that each DHHS division and office assign an Identity Theft Coordinator to investigate and report inappropriate disclosures of identifying information. This same Identity Theft Coordinator will also be responsible for recording, investigating and reporting incidents involving covered account red flags, address discrepancies and debit/credit card accounts.

Each division and office shall implement a process for investigating, mitigating and reporting incidents timely. If an incident occurs, the Identity Theft Coordinator shall notify the DHHS Privacy Officer immediately and forward the results of the investigation to the DHHS Privacy Officer when the investigation has been completed.

The Identity Theft Coordinator shall also submit a list of his or her division’s or office’s incidents to the DHHS Privacy Officer no later than December 31st of each year, providing a brief description of the incident, the date the incident occurred, and the resolution of the incident.

F. Respond to the receipt of a notice of address discrepancy from a consumer reporting agency

A division or office that uses consumer reports must develop and implement reasonable policies and procedures designed to enable it to form a reasonable belief that a consumer report relates to the client about whom it has requested the report, when the division or office receives a notice of address discrepancy.

Examples of reasonable policies and procedures are:

- Comparing the information in a consumer report provided by the consumer reporting agency with information the division or office:

- Obtains and uses to verify the consumer’s identity in accordance with the requirements of the Customer Information Program (CIP) rules implementing 31 U.S.C. 5318(l),
 - Maintains in its own records, such as applications, change of address notifications, other customer account records, or retained CIP documentation; or
 - Obtains from third-party sources; or
- Verifying the information in the consumer report provided by the consumer reporting agency with the client.

The division or office must also develop and implement policies and procedures to reasonably confirm the accuracy of a consumer address that will be furnished to the consumer reporting agency from whom it received a notice of address discrepancy, when the division or office:

- Can form a reasonable belief that the consumer report relates to the client about whom the division or office requested the report;
- Has a continuing relationship with the client; and
- *Regularly and in the ordinary course of business*, furnishes information to the consumer reporting agency that sent the notice of address discrepancy.

NOTE: *The notification requirement exists only if a division or office regularly supplies information to the consumer reporting agency, and the confirmed address can be included in the division’s or office’s next regularly scheduled delivery of information to that consumer reporting agency.*

G. *Reasonably confirming that an address is accurate*

The division or office may reasonably confirm that an address is accurate by:

- Verifying the address with the client about whom it has requested the report;
- Reviewing its own records to verify the address of the client;
- Verifying the address through third-party sources; or
- Using other reasonable means.

NOTE: *The Federal Trade Commission (FTC) is interpreting this requirement as only applying to notices of address discrepancies on consumer reports, also known as credit reports, issued by nationwide consumer reporting agencies (“CRAs”), as defined in Section 603(p) of the Fair Credit Reporting Act (“FCRA”). Today, the FTC staff has stated there are only three such nationwide CRAs: Experian, TransUnion and Equifax. Therefore, as a practical matter, notices of address discrepancy on consumer reports issued by the “big three” entities (directly or through intermediaries) are the reports that the FTC staff believes are currently subject to this rule.*

The FTC has stressed that the obligation to conduct address verification only applies to a user of the consumer report that has received a “notice of address discrepancy” from one of the three nationwide CRAs. In other words, in the FTC staff’s view, users of consumer reports, such as nursing homes, assisted living facilities or other health care entities, that may use consumer reports for employment or admissions purposes, are only technically required to perform the address verification upon receiving such an express “notice of address discrepancy.”

References:

Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003, 16 CFR Part 681

Identity Theft and Security Breach Notification Policy, DHHS Policy and Procedures Manual, Section VIII. Privacy and Security, Privacy Manuals, Identity Theft Policies

Customer Information Program (CIP), 31 U.S.C. 5318(l)

www.ftc.gov/redflagrule

Red Flag and Address Discrepancy Requirements: Suggestions for Health Care Providers, The World Privacy Forum, Robert Gellman and Pam Dixon, September 24, 2008

Appendices:

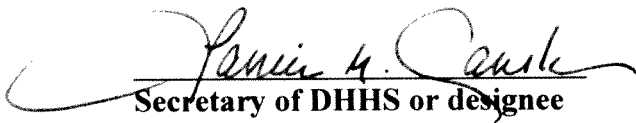
Appendix A: DHHS Red Flag and Address Discrepancy Assessment Questionnaire

Appendix B: Red Flags

Appendix C: Red Flags in a Health Care Setting

DHHS Red Flag and Address Discrepancy Policy

Per the Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003, 16 CFR Part 681, the Red Flag and Address Discrepancy Policy has been approved for implementation within the NC Department of Health and Human Services (DHHS).


Secretary of DHHS or designee

7/28/09
Date

APPENDIX A

DHHS Red Flag and Address Discrepancy Assessment Questionnaire

In order for a North Carolina (NC) Department of Health and Human Services (DHHS) division or office to determine whether the Red Flag Rule applies to its business operations and if Identity Theft Prevention Program procedures must be developed, the division or office must ask itself the following questions:

Question 1: Is your division or office a creditor or a financial institution?

If **NO**, Go to Question 3.
If **YES**, Go to Question 2.

Question 2: Does your division or office offer or maintain covered accounts?

If **NO**, Go to Question 3.
If **YES**, Develop procedures as part of DHHS Identity Theft Prevention Program. Go to Question 3.

Question 3: Does your division or office order credit reports on consumers from a Consumer Reporting Agency?

If **NO**, Go to Question 4.
If **YES**, Develop procedures on how you will determine if your client's address has changed, after receiving a notice of address discrepancy from the consumer reporting agency. Go to Question 4.

Question 4: Does your division or office issue debit or credit cards?

If **NO**, Go to Question 5.
If **YES**, Develop procedures on how you will assess the validity of a change of address if you receive notification of a change of address for a debit/credit card account and within a short period of time afterwards, you receive a request for an additional or replacement card for the same account. Go to Question 5.

Question 5: Is your division or office a service provider for a DHHS division or office that is subject to the Red Flag and Address Discrepancy Rules?

If **NO**, .
If **YES**, Go to Question 6.

Question 7: Is the service your division or office provides to the DHHS division or office covered by the Red Flag and/or Address Discrepancy Rules?

If **NO**, .

If **YES**, Develop the applicable procedures based upon the service provided to the DHHS division or office.

APPENDIX B

Red Flags

from a Consumer Reporting Agency

1. A fraud or active duty alert is included with a consumer report.
2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.
3. A consumer reporting agency provides a notice of address discrepancy, as defined in § 334.82(b) of Part 681.
4. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:
 - a. A recent and significant increase in the volume of inquiries;
 - b. An unusual number of recently established credit relationships;
 - c. A material change in the use of credit, especially with respect to recently established credit relationships; or
 - d. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

Suspicious Documents

5. Documents provided for identification appear to have been altered or forged.
6. The photograph or physical description on the identification document is not consistent with the appearance of the applicant or customer presenting the identification.
7. Other information on the identification document is not consistent with information provided by the person opening a new covered account or customer presenting the identification.
8. Other information on the identification document is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check.
9. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Suspicious Personal Identifying Information

10. Personal identifying information provided is inconsistent when compared against external information sources used by the financial institution or creditor. For example:

- a. The address does not match any address in the consumer report; or
 - b. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.
11. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.
 12. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:
 - a. The address on an application is the same as the address provided on a fraudulent application; or
 - b. The phone number on an application is the same as the number provided on a fraudulent application.
 13. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:
 - a. The address on an application is fictitious, a mail drop, or prison; or
 - b. The phone number is invalid, or is associated with a pager or answering service.
 14. The SSN provided is the same as that submitted by another person opening an account or another customer.
 15. The address or telephone number provided is the same as or similar to the address or telephone number submitted by an unusually large number of other persons opening accounts or other customers.
 16. The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.
 17. Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor.
 18. For financial institutions and creditors that use challenge questions, the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

Unusual Use of, or Suspicious Activity Related to, the Covered Account

19. Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for new, additional, or replacement cards or a cell phone, or for the addition of authorized users on the account.
20. A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example:
 - a. The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry); or
 - b. The customer fails to make the first payment or makes an initial payment but no subsequent payments.
21. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example
 - a. Nonpayment when there is no history of late or missed payments;
 - b. A material increase in the use of available credit;
 - c. A material change in purchasing or spending patterns;
 - d. A material change in electronic fund transfer patterns in connection with a deposit account; or
 - e. A material change in telephone call patterns in connection with a cellular phone account.
22. A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).
23. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.
24. The financial institution or creditor is notified that the customer is not receiving paper account statements.
25. The financial institution or creditor is notified of unauthorized charges or transactions in connection with a customer's covered account.

Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection with Covered Accounts Held by the Financial Institution or Creditor

26. The financial institution or creditor is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

APPENDIX C

Situations that could alert a creditor that an identity theft incident may be in progress or has already occurred in a health care setting

1. A complaint or question from a patient based on the patient's receipt of:

- a bill for another individual;
- a bill for a product or service that the patient denies receiving;
- a bill from a health care provider that the patient never patronized; or
- an Explanation of Benefits or other notice for health services never received.

An unexpected bill or notice of benefits can be one way that a patient can learn that she has been a victim of medical identity theft. "Explanations of Benefits" (EOB) are potentially important tools for patients and providers. For example, hotline information to report possible fraudulent or suspicious activity can be included on an EOB.

2. Records showing medical treatment that is inconsistent with a physical examination or medical history as reported by the patient. In particular, records that show substantial discrepancies in age, race, and other physical descriptions may be evidence of medical identity theft. An incorrect blood type is evidence that the patient was a victim of medical identity theft.
3. A complaint or question from a patient about the receipt of a collection notice from a bill collector. A collection notice can be one way that a patient can learn that she has been a victim of medical identity theft.
4. A patient or insurance company report that coverage for legitimate hospital stays are being denied because insurance benefits have been depleted, or that a lifetime cap has been reached. Members of a family can be victimized by "looping", where a thief uses one family member's benefits and then turns to the next family member when the first victim's benefits have run out.
5. A complaint or question from a patient about information added to a credit report by a health care provider or insurer. An entry in a credit report can be one way that a patient can learn that she has been a victim of medical identity theft.
6. A dispute of a bill by a patient who claims to be the victim of any type of identity theft. Although financial identity theft differs significantly from medical identity theft, a victim of financial identity theft may be more likely to also be a victim of medical identity theft. Victims of financial identity theft may have filed police reports about their case, and these need to be taken into account.
7. A patient who has an insurance number but never produces an insurance card or other physical documentation of insurance. A medical identity thief may succeed by obtaining the medical insurance number and other information about the victim. The absence of an actual insurance

card is evidence suggesting that the person being treated may not be the actual insured. Note: This particular Red Flag has to be applied with caution because there are other reasons a patient may not have her insurance card.

8. A notice or inquiry from an insurance fraud investigator for a private insurance company or a law enforcement agency. Not all forms of medical identity theft are the result of an individual thief presenting for treatment. Fraudulent billing by a physician can result in false information in a health record that may affect the treatment of patients. In some cases, clerks, nurses and other hospital employees have exploited their legitimate access to health files to use patients' identity and health information for medical identity theft.