TO: Steve Hess
Chief Information Officer
University of Utah

FROM: Chris Kidd
OIT Compliance Office

RE: Guidelines for University Compliance with the Fair and Accurate Credit Transaction Act of 2003's Red Flag Rules

DATE: April 21, 2009

I have attached the guidelines that are required by University Policy, "Identity Theft Prevention Program." These guidelines were published by the Federal Trade Commission (FTC). The University Policy requires departments with covered accounts (as defined in the policy) to "review the guidance and update [internal] policies and procedures relevant to their operations, to reflect changes in risk" based on this, or updated, guidance.

Sample Plan

A sample plan, based on the guidance, is listed below:

Department ABC allows individuals to pay for services on a payment plan. The individual must fill out an application and undergo a credit check. Department ABC has read over the guidance and determined the following are reasonable and appropriate methods of implementing the policy:

Detecting/Preventing Identity Theft
Department ABC will:

- Review the following items, routinely included in credit reports:
  - A fraud or activity duty alert;
  - A notice of credit freeze; and
  - A notice of address discrepancy.
- Request identification and:
  - Ensure the identification is not forged or altered; and
  - Ensure the ID is consistent with the appearance of the consumer who is presenting the identification.
- Ensure the completed application has not been altered, or destroyed and reassembled.

Responding to and Mitigating Identity Theft
If Department ABC suspects, or has knowledge of, identity theft, they will:

- Attempt to contact the correct individual to notify them of the issue;
- Consult with the Office of General Counsel prior to notifying law enforcement; and
- Notify the Information Security and Privacy Office.

Identity Theft Guidelines

These guidelines have been developed as required by the Identity Theft Risk Reduction policy. It outlines methods for detecting, preventing, responding to, and mitigating identity theft. These guidelines will be updated as risks change.

Departments are NOT required to implement all of these items. These items are to be used as guidelines for departments to develop reasonable and appropriate internal policies and procedures to detect, prevent, respond to, and mitigate identity theft.

Additional Information on Applicability

Please note that gift cards, or other prepaid cards, have been specifically *exempted* by the FTC from these requirements (see Rule 04-004, definition of 'covered account.').

Definitions used in these Guidelines

Consumer Reporting Agency means an agency which collects and sells information about the creditworthiness of individuals (also called a credit bureau).

Member means a patient, student, faculty member, volunteer, or other individual utilizing a covered account at the University.

Phishing means using e-mail, the web, or other electronic forms of communication in a criminal manner to obtain usernames, passwords, or other information. For example, end-users may receive e-mails that appear to be from their bank, but are actually forgeries used to collect account numbers and PINs.

I. **Consider the Following For Purposes of Detecting or Preventing Actual Risk for Identity Theft:**

These guidelines are extensive and may not apply to all departments. Please review these guidelines and adopt policies and procedures *where applicable*.

A. Alerts, notifications, or other warnings received from a Consumer Reporting Agency or service providers: The alerts, notifications, or other warnings include, but are not limited to:

1. A fraud or activity 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;
4. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or member;
5. The credit report or use of the account that indicates a pattern of activity is inconsistent with the history or pattern of activity usually associated with the member, 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 institutions or creditor.

B. Presentation of suspicious documents: This may include, but not limited to:

1. Documents provided for identification appear to be forged or altered;

2. The photograph, description of the consumer, or other information on the identification is inconsistent with the appearance of the consumer who is presenting the identification;
3. Other information on the identification is not consistent with the information on the identification provided by the person when the account is opened or by the consumer presenting the identification.;
4. Other information provided is inconsistent with information on file; or
5. An application appears to be altered, or destroyed and reassembled.

C. Presentation of suspicious personal identifying information, such as a suspicious address change: This may include, but is not limited to:

1. Personal information provided is inconsistent when compared to external information sources, such as:
   a) The address does not match any address in the credit report; or
   b) The SSN has not been issued, or is listed on the Social Security Administration's Death Master File.
   c) Personal information is internally inconsistent, such as an SSN that is inconsistent with a consumer's date of birth;
   d) Personal information is provided that has also been provided on a fraudulent application;
   e) Personal information that is provided is of a type associated with fraudulent activity, such as a fictitious address (i.e., mail drop or a prison) and an invalid phone number (i.e., pager or answering service);
   f) The address, SSN, and phone numbers have been submitted by other consumers;
   g) The consumer fails to provide all required information on an application;
   h) Personal information is not consistent with information on file; or
   i) The consumer cannot provide authenticating information, other than what would be available from a wallet or credit report.

D. The unusual use of, or other suspicious activity related to, a covered account: This may include, but is not limited to:

1. An account is used in a manner inconsistent with established patterns of activity, such as nonpayment when there is no history of late or missed payments;
2. Mail sent to the member is returned repeatedly as undeliverable even though transactions on the account continue to be conducted;
3. We are notified that we have opened a fraudulent account for a person engaged in identity theft.

E. Notice from members, ID Theft victims, law enforcement, or other persons regarding possible ID Theft: We are notified by a:

1. Member;
2. Victim of ID Theft;
3. Law Enforcement Authority; or
4. Any other person that it has opened a fraudulent account for a person engaged in ID Theft.

F. Departments should apply procedures and processes in detecting Red Flags in connection with the opening of covered accounts and existing covered account, such as:

1. Cross referencing other operating policies and procedures for obtaining identifying information about, and verifying the identity of, a person opening a covered account.

2. Cross referencing the detection of Red Flags in connection with existing covered accounts by Validating Change of Address.

G. Departments which utilize e-mail are highly encouraged to implement anti-spam/anti-phishing technology to help eliminate precursors to identity theft such as collection of information by e-mail.

II. **Responding to Detection of, and Mitigating, Identity Theft**

A. *As always, the safety of our patients, staff, visitors, and others comes first*. Please keep this in mind when reviewing these guidelines and adjusting your internal policies and procedures. It may not be appropriate (or safe), based on the context of the situation, for a department to challenge an individual.

B. If identity theft is detected, departments must notify the Information Security and Privacy Office within one business day. One, or more, of the following steps may be taken:

1. Monitoring a "covered account" for evidence of Identity Theft;
2. Contacting the Patient/Member;
3. Asking the Patient/Member to review their medical records or insurance records to ensure they are accurate;
4. Changing any password, security codes, or other security devices;
5. Reopening a covered account with a new account number;
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 circumstance(s).