

THE RED FLAG RULES



Presented by
C'Shalla Parker
University Privacy Officer

Introduction



- Fair and Accurate Transaction Act (FACTA)
 - Congress – Federal Trade Commission and other
Other agencies to develop regulation requiring “creditors” and
“financial institutions” to address risk of identity theft.

Introduction



- November 9, 2007
 - FTC and other agencies issued regulations that require the detection, prevention and mitigation of identity theft – RED FLAGS RULE
 - November 1, 2008 – Original Effective Date
 - Postponed to May 1, 2009 and again until
 - August 1, 2009.

Requirement of the Red Flag Rule



- Financial institutions and creditors with covered accounts must establish an identity theft prevention program to identify RED FLAGS and to prevent and mitigate identity theft.

Creditor



- FACTA's definition of a creditor is extremely broad and includes all entities that regularly permit payments for goods and services. However, accepting credit cards as a form of payment does not, by itself, make an entity a creditor.

Covered Account



- Any other account that the financial institution or creditor offers or maintains for which there is a reasonable foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft.

Creditor



- UTMC is a creditor because...
 - it regularly bills patients after the completion of services, including for the remainder of medical fees not reimbursed by insurance.
 - it regularly sets up payment plans after services have been rendered.

RED FLAG

- The Red Flag Rule defines Identity Theft as
 - A pattern, practice, or specific activity that indicates the possible existence of identity theft.



What is Identity Theft?

- Occurs when someone uses another person's identifying information without permission to commit fraud or other crimes
 - This information could include:
 - Name
 - SSN
 - Insurance Number
 - Credit Card Number
 - Potential Consequences
 - False Diagnosis
 - Unsafe care or deadly care
 - Future denials of insurance coverage



What can employees do?

- Be alert and considerate of everyone by implementing:
 - Safeguards to prevent identity theft
 - Procedures to detect suspicious activities
 - Reporting procedures when suspected identity theft has occurred.



How to Prevent, Detect, and Report



- Create a program to prevent, detect, and report Identity Theft to reduce the harmful effects of Identity Theft such as:
 - A policy dedicated to identity theft
 - Education on Red Flag – Fraud Alerts
 - A Red Flag Committee
 - An Identity Theft Response Team for Investigations

Prevention

- Always use shredders for confidential/PHI information
 - Keep passwords secure and do not share them
 - Eliminate the use of SSN wherever it is possible
-
- 3364-15-12 Identity Theft Prevention, Detection, and Mitigation <http://www.utoledo.edu/policies>



Detection

- Detecting Identity Theft Red Flags is dependent on awareness of suspicious activities common to the department where you work.



Be Proactive

- If you think of additional Identity Theft Red Flags common to your department share them with your supervisor to raise awareness for your department!



Reporting

- Identity Theft must be reported as soon as it is suspected!
 - Contact manager
 - Contact University of Toledo Police Department

Do not delay emergency treatment




FTC Affidavit

• A patient may contact UTMC after being a victim of Identity Theft.

• They may complete the Passport Program offered by the Federal Trade Commission.

• This form is available at:

<http://www.ftc.gov/bcp/edu/microsites/idtheft/>


PASSPORT PROGRAM
RICHARD CORDRAY, OHIO ATTORNEY GENERAL

INSTRUCTIONS FOR COMPLETING THE ID THEFT AFFIDAVIT

To make certain that you do not become responsible for the debts incurred by the identity thief, you must provide proof that you did not create the debt to each of the companies where accounts were opened or used in your name.

A working group composed of credit grantors, consumer advocates and the Federal Trade Commission (FTC) developed this *ID Theft Affidavit* to help you report information to many companies using just one standard form. Use of this affidavit is optional for companies. While many companies accept this affidavit, others require that you submit more or different forms. Before you send the affidavit, contact each company to find out if they accept it.

You can use this affidavit where a new account was opened in your name. The information will enable the companies to investigate the fraud and decide the outcome of your claim. (If someone made unauthorized charges to an existing account, call the company to find out what to do.)

This affidavit has two parts:

- *ID Theft Affidavit* is where you report general information about yourself and the theft.
- *Fraudulent Account Statement* is where you describe the fraudulent account(s) opened in your name. Use a separate *Fraudulent Account Statement* for each company you need to write to.

When you send the affidavit to the companies, attach copies (NOT originals) of any supporting documents (e.g., driver's license, police report) you have. Before submitting your affidavit, review the disputed account(s) with family members or friends who may have information about the account(s) or access to them.

Complete this affidavit as soon as possible. Many creditors ask that you send it within two weeks of receiving it. Delaying could slow the investigation.

Be as accurate and complete as possible. You may choose not to provide some of the information requested. However, incorrect or incomplete information will slow the process of investigating your claim and absolving the debt. Please print clearly.

When you have finished completing the affidavit, mail a copy to each creditor, bank or company that provided the thief with the unauthorized credit, goods or services you described. Attach to each affidavit a copy of the *Fraudulent Account Statement* with information only on accounts opened at the institution receiving the packet, as well as any other supporting documentation you are able to provide.

Send the appropriate documents to each company by certified mail, return receipt requested, so you can prove that they were received.

The companies will review your claim and send you a written response telling you the outcome of their investigation. Keep a copy of everything you submit for your records.

If you cannot complete the affidavit, a legal guardian or someone with power of attorney may complete it for you. Except as noted, the information you provide will be used only by the company to process your affidavit. Investigate the events you report and help stop further fraud. If this affidavit is requested in a lawsuit, the company might have to provide it to the requesting party.

Completing this affidavit does not guarantee that the identity thief will be prosecuted or that the debt will be cleared.

Page 1 of 7

**DO NOT SEND AFFIDAVIT TO THE FTC
OR ANY OTHER GOVERNMENT AGENCY**

This project was supported by Grant No. 2006-VI-CJ-002 awarded by the Office for Victims of Crime, Office of Justice Programs, U.S. Department of Justice.
Points of view in this document are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice.
Affidavit - Updated 04-08

Contact Information

- Contact your supervisor
- Contact the Compliance Office
 - C'Shalla Parker University Privacy Officer
419-383-4270



Examples of Red Flags



- **Suspicious Personal ID info**

- Info presented inconsistent with external info
- Info presented inconsistent with info on file
- ID associated with known fraud activity or previous red flag
- Duplicate ssn
- Duplicate medicaid card
- Duplicate address or telephone #
- Incomplete info
- Person unable to authenticate presented info

- **Suspicious Activity**

- New or replacement request shortly following address change
- Usage consistent with known fraud patterns
- Unusual usage, inconsistent with normal patterns
- Mail returned despite continued confirmation of address
- Person complains about receiving a bill denying receipt of services

Examples Cont.

- **Suspicious Medical Information**

- Person presents medical background inconsistent with existing medical record
- Person unaware of basic medical background
- Medical record inconsistent with physical examination of patients account of medical history
- Person's insurance company report that coverage for legitimate hospital stay is denied because benefits have been depleted
- Person denies info provided in medical record
- Lab (blood work, type etc) inconsistent with info in medical record
- Person refuses to provide insurance card

- **Suspicious Documentation**

- Altered/forged ID
- Inconsistent photo/description
- ID info doesn't match what is on file
- Altered/forged application



WHAT IS A RED FLAG?

- RED FLAG A
- RED FLAG B
- RED FLAG C
- RED FLAG D
- RED FLAG E

Resources



- Federal Trade Commission-Identity Theft
 - <http://www.ftc.gov/bcp/edu/microsites/idtheft/>
- Attorney General's Office-Identity Theft
 - <https://www.ohioattorneygeneral.gov/IdentityTheft>

RED FLAG



THANK YOU!