THE RED FLAG RULES

Presented by
C'Shalla Parker
University Privacy Officer

New Regulations

- There are new federal regulations related to identity theft with which the University must comply.
- This presentation is designed to help staff understand their role in preventing, detecting, and reporting identity theft.

Objectives

- To educate staff on the following topics:
  - Identity Theft
  - Identity Theft Red Flag Rules
  - Identity Theft Program: Prevent, Detect, and Report Identity Theft

Identity Theft

- Occurs when someone uses another person's identifying information without permission to commit fraud or other crimes.
- Identifying information may include:
  - Name;
  - Social security number
  - Medical insurance number
  - UT Rocket ID badge
  - Credit card number

Consequences of Identity Theft

- There are potentially dangerous consequences to identity theft.
  - Loss/negative affect to credit
  - High expenditures to credit cards
  - Civil/Criminal charges to pursue
  - Extended time frame to regain credit and identity

Red Flag Rules

- The Federal Trade Commission has created regulations known as the Identity Theft Red Flag Rules.
- Under these rules The University of Toledo must create a program to prevent, detect, and reduce the harmful effects of identity theft.

Red Flag Rules

- The new rules define an Identity Theft Red Flag as a pattern, practice, or specific activity that indicates the possible existence of identity theft.

Prevent-Detect-Report

- To prevent, detect, and report Identity Theft Red Flags, the University has:
  - A policy dedicated to identity theft
  - An Identity Theft Response Team
  - Standard Operating Procedures for areas where identity theft most often presents such as;
    - Registrar
    - Financial Aid
    - Bursar

Prevent-Detect-Report

- On a daily basis , staff must:
  - Prevent identity theft from occurring by safeguarding information;
  - Detect identity theft by being aware of suspicious activities; and
  - Report identity theft as soon as you suspect it.

Prevent

To help prevent identity theft, staff members must;

- 3364-15-12 Identity Theft Prevention, Detection, and Mitigation http://www.utoledo.edu/policies

- Place all confidential documents in shredders
- Maintain electronic security by using strong passwords and never sharing them
- Be alert to identity theft triggers common in the area where you work; and
- Be aware of your department specific procedures related to identity theft

Detect

- To detect identity theft, you must be aware of suspicious activity or Identity Theft Red Flags common to the University and the department where you work.
  - Some Identity Theft Red Flags the University has identified include:
    - A complaint or question from a student based on the student's receipt of;
      - A bill for another student
      - A bill for a product or service the student did not receive
      - A notice regarding grades or
      - A collection notice from a collection agency

Other Examples

- Documents provided for identification appear altered or forged
- The photograph on the identification does not resemble the person presenting the identification at the time of appointment or purchase
- Complaint or questions from a student or customer about information added to a credit report.

Be Proactive

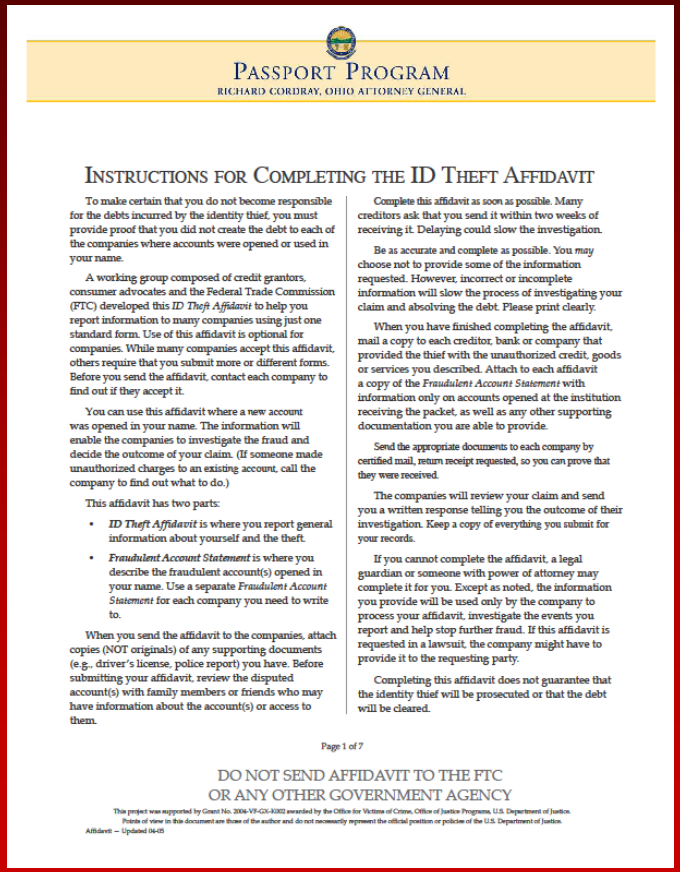
- If you think of additional Identity Theft Red Flags common to your department share them with your supervisor to raise awareness for your department!

Reporting

- Identity Theft must be reported as soon as it is suspected!
  - Contact manager
  - Manager will contact Privacy Officer/Security Officer

FTC Affidavit

- A student may contact the University 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-VF-GX-K002 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.

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 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 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!