ID Theft Red Flags Policy at CMU

2009

Statutory Provisions Implemented

- The Fair and Accurate Credit Transactions Act of 2003 (FACT Act) amended the Fair Credit Reporting Act (FCRA)

- Sections 114 and 315 of the FACT Act

Rules: 72 Fed. Reg. 63718 (November 9, 2007)
http://www.ftc.gov/os/fedreg/2007/november/071109redflags.pdf

Purpose of the Red Flags Rule

- To detect and stop identity thieves using someone else's identifying information at your institution to commit fraud.
- Distinct from data security
  - CMU has a separate Data Security Policy
  - Located with the rest of CMU's administrative policies

Covered Entities

"Financial institutions" and "creditors" must conduct a periodic risk assessment to determine if they have "covered accounts."

Definitions

From the FCRA, a "financial institution" is, among other things:

- Any other person that directly or indirectly holds a transaction account* belonging to a consumer – this includes CMU

* From the Federal Reserve Act, Sec. 19(b) - an account that allows withdrawals by negotiable or transferable instrument, payment orders of withdrawal, telephone transfers, or similar items to make payments or transfers to 3rd persons or others.

Definitions (cont'd)

A "creditor" is:

- Any person who regularly extends, renews, or continues credit
- Any person who regularly arranges for the extension, renewal, or continuation of credit, or
- Any assignee of an original creditor who participates in the decision to extend, renew, or continue credit

Definitions (cont'd)

A "covered account" is:

- A consumer account designed to permit multiple payments or transactions, and
- Any other account for which there is a reasonably foreseeable risk from identity theft

Legal Requirement

covered accounts must implement a written Identity Theft Prevention Program to *detect*, *prevent*, and *mitigate* identity theft in connection with:

- the opening of a covered account, or
- any existing covered account

CMU's Response

- CMU's Board of Trustees approved an ID Theft Red Flags Policy at its April meeting

Elements of CMU's Program

Includes reasonable policies and procedures to:

- Identify relevant red flags* and incorporate them into the Program
- Detect red flags that are part of the Program
- Respond appropriately to any red flags that are detected
- Ensure the Program is updated periodically to address changing risks

* A red flag is a pattern, practice, or specific activity that could indicate identity theft

CMU Offices that maintain covered accounts (Page 1)

- Academic Advising (orientation)
- Admissions
- Athletics
- CMU Police
- University Recreation
- Educational Materials Center
- Central Mailroom
- Beaver Island
- Bookstore
- CARLS Center
- Central Box Office/University Events
- Development
- Gay and Lesbian Programs
- Graduate Studies
- HEV
- Honors Program
- Human Development Clinic
- Health Services

CMU Offices that maintain covered accounts (Page 2)

- IT
- Office of International Education
- ProfEd
- Public Broadcasting
- Public Relations and Marketing
- Scholarships and Financial Aid
- Receivable Accounting
- Residence Halls
- Recreation, Parks, & Leisure Services Administration
- School of Music
- Special Olympics
- Student Publications
- Teacher Education and Professional Development
- Telecom
- Others?

Service Provider (Non-CMU) Covered Accounts

- UAS
- Money Network (Meta Bank)
- GRC
- Recovery Management Services
- American Collection Systems
- Nelnet Business Solutions

Program Definitions

- **Identity Theft** – fraud committed or attempted using the identifying information of another person without authority
- **Sensitive Information** – account information that, if obtained, could lead to the commission of ID theft
- **Covered Accounts** – at CMU, those accounts that permit multiple payments or transactions
- **Red Flag** – pattern, practice, or specific activity that indicates possible ID theft

Types of Sensitive Information

- Credit Card Information
- Tax ID numbers
- Payroll Information
- Cafeteria Plan check requests
- Medical Information
- Other personal information, including dates of birth, address, phone number, photos, etc.

Risk Factors in Identifying Red Flags

- Types of covered accounts as noted above (previous slide)
- Methods provided to open covered accounts
  - Application
  - High school transcripts
  - ACT/SAT scores
  - Medical records/immunization history
  - Insurance card

Risk Factors in Identifying Red Flags

- Methods provided to access covered accounts
  - Phone
  - Email/internet
  - Non face-to-face
- CMU's previous history, if any, with ID theft

Program-Identified Red Flags

- Documents provided for identification appear to have been altered or forged
- Photograph or description on ID is inconsistent with appearance of person presenting it
- A request pertaining to the account is made from a non-CMU issued email account
- There is a request to mail information contained in a covered account to an address not listed on file
- We receive notice of possible ID theft in connection with a covered account, or alerts from a credit reporting or monitoring agency

Responses to Red Flags

- Deny access to the covered account until other information is available to eliminate the red flag
- Contact the person affected
- Change any passwords or other means of accessing the covered account
- Notify law enforcement (if appropriate) OR
- Determine no response is warranted

What if you find a Red Flag?

- Report to the office of the AVP for Financial Services and Reporting (774-3331)
- They will review the report and determine what steps, if any, should be taken
- They will communicate with your office how to proceed
- They will also periodically review and update the Program

Incident Report Form

- Available from Financial Services and Reporting
- **Suspected Red Flag Rules Incident Report Form**
  - Victim Name:
    Campus ID number:
  - Date of suspected theft:
  - Person reporting suspected theft:
    Date:
  - Please provide a summary of the suspected theft (including any steps taken, such as placing holds on accounts, etc.):
  - Has the suspected victim of theft been contacted?

How do I Keep it all Straight?????

- Ask yourself the following:
  - Do I maintain/have access to a **COVERED ACCOUNT?**
  - That contains **SENSITIVE INFORMATION?**
- If no to the above, YOU ARE IN THE WRONG TRAINING AND YOU CAN LEAVE RIGHT NOW!!!
- If **YES**, ……..

Are any of the Following Risk Factors Present?

- Accounts contain **SENSITIVE INFORMATION**
- **SENSITIVE INFORMATION** was used to open the account
- **REMOTE ACCESS** to the covered account is permitted
- There is a **PREVIOUS HISTORY** of ID theft relative to the covered account
- **If YES, ….**

Watch for these RED FLAGS

- ID documents appear to have been **forged**
- **Photos** do not match appearance
- Request made from **NON-CMU** email account
- Mail to address **not on file**
- **Previously received** notices of possible ID theft
- **Alerts** from credit monitoring agencies

- If **YES** to any of the above….

REPORT IT!!!!!!!!!

- REPORT TO FINANCIAL SERVICES AND REPORTING AT 774-3331
- Use Incident Report Form (available from Financial Services and Reporting)
- You will be contacted if additional follow up is required

Responses that will be considered

- **DENY** access to account
- **CHANGE** passwords/access methods
- **CONTACT** affected individual
- **REPORT** to law enforcement; OR
- Determine **NO RESPONSE** is warranted

QUESTIONS????

Contact General Counsel's office at 989-774-3971