

Protecting Confidential and Sensitive Information

Red Flag Regulations

Overview of Topics

- Identity Theft Put In Context
- Red Flag Regulations Overview
- How UM Protects Information
- What is the Student Workers role in identity theft prevention?



What's this all about?

- Why is UM concerned about identity theft?
 - The University of Montevallo is subject to federal rules regarding security because we offer or participate in:
 - Student tuition and fee payment plans
 - The Federal Perkins Loan program
 - Other payments through various departmental programs on campus such as Child Study Center, Community School of Music, etc.



Identity Theft Put In Context

What is Considered Identity Theft?

- Identity theft takes place when key pieces of personal identifying information is stolen.
- This can include:
 - Drivers Licenses Numbers
 - Social Security Numbers
 - Credit Card Accounts
 - Other personal information



Why is training on identity theft prevention important?

- Between January 2005 and June 2008, 227,205,625 records were compromised from US government agencies, businesses, schools, and other organizations.

Privacy Rights Clearinghouse, 2008

- The total one year amount of identity fraud in 2006 cost \$55.7 billion.

Javelin Strategy & Research Survey, 2007



Common Causes

Internal Threats

Poorly trained personnel

Inadequate security measures

Insufficient support from management

Unsupervised third party providers

Dishonest insiders

Inadequate IT systems

Human error

External Threats

Hackers

Organized crime

Social engineers

Competitors

Common Methodology

- Dumpster Diving
- Eavesdropping
- Family, Friends, Co-workers
- Hacking
- Insiders
- Mail Theft
- Name Dropping

- Pharming
- Phishing
- Piggy Backing
- Pretexting
- Shoulder Surfing
- Skimming
- Social Engineering
- War Driving

Bottom Line For You As A Student Worker

- Perhaps the greatest cause of information loss or breach is the **HUMAN ELEMENT**.

“From an organization’s perspective, people include employees, customers, third parties, and business partners. All of these people are vital to the organization’s survival and are privy to the organization’s information in varying degrees through different means.

As a result, all of these PEOPLE PRESENT RISK. Well aware that infrastructures and perimeters have been fortified, today’s sophisticated crooks no longer batter the fortress directly – they take a subtler approach through its people.”

Deloitte 2007 Global Security Survey: The Shifting Security Paradigm

Red Flag Regulations

Federal rules UM employees must follow regarding identity protection

Red Flag Regulations

- The Red Flag Regulations & Guidelines come from
 - Sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACTA) of 2003 passed in October 2007

The Federal Trade Commission governs and enforces this regulation.



Red Flag Regulations

- What's the Purpose?
 - Financial institutions and creditors must:
 - Develop and implement an Identity Theft Prevention program to detect, prevent, and mitigate identity theft in connection with the opening of certain accounts or certain existing accounts.



Why Does This Apply To Me?

- UM extends credit to students in the form of financial aid and payment plans.
- According to the Red Flag Rules, that makes staff at UM (even student staff) responsible for following the Red Flag Rules when dealing with confidential and sensitive information.



What is Confidential and Sensitive Information?

- Any one piece of information with a person's or company's name beyond the information you would find in a phone directory or on a business card
- As a member of UM staff you could handle this type of information.



If you work with information from sources such as:

- Financial Accounts
- Medical Accounts
- Employment Accounts
- Education Accounts
- Criminal or Student Judicial Accounts

You will be handling confidential and sensitive
information (CSI)

Defining Confidential and Sensitive Information (CSI)

Personal Information

- Social Security Number
- Social Insurance Number
- Birth Dates
- Driver's License Information
- Professional License Information
- Student Id numbers such as M#

Business Information

- Federal ID Numbers
- Proprietary Information
- Trade Secrets
- Business Systems
- Student ID's
- Access Numbers /Passwords
- Customer Identifiers, Vendor Numbers, and Account Numbers

Financial Information

- Credit Card Numbers
- Expiration Dates of Cards
- CCV Numbers from Cards
- Bank/Credit Union Account Number
- Credit Reports
- Billing Information
- Payment History

Medical Information

- Medical Records
- Doctor Names and Claims
- Health, Life, Disability Insurance Policy Information

How UM Protects Information

Protective Measures for...

- Data Security

Know where sensitive files are located and used

Keep only what is needed and dispose of everything else

Lock up sensitive information

Shred papers with identifying information

Report security breaches to your supervisor immediately

<http://business.ftc.gov/documents/bus69-protecting-personal-information-guide-business.pdf>



Protective Measures for...

- Student Privacy

Protecting a student's privacy is just as important as protecting his or her data.

- Never give out private information on other students
- This includes:
 - Parents
 - Friends
 - Co-Workers from other departments (unless directed by your direct supervisor)

Safety Concerns

- Never give out individual addresses, room numbers, or class schedules to the public
- Parents are included in the public realm
- Refer parents to your supervisor if they are asking for information you cannot release



Protective Measures for...

- Employee Privacy and Security

Providing security and privacy for employees helps protect everyone.

- Place your personal items, such as bags, in a secure area.
- When speaking on the phone be aware of who may overhear what you are disclosing. If necessary, transfer the call to a more secure environment.
- Secure office computers with a password at the end of your shift.

**What is a Student
Worker's role in identity
theft prevention?**

Basic Requirements for Student Workers

- As a student worker at UM
 - You are expected to follow basic rules for keeping information private such as:



Basic Rules for Student Workers

- As a student worker at UM
 - You are expected to follow basic rules for keeping information private such as:

Shredding waste paper that has confidential and sensitive information

Securing your desk and computer before leaving your station

Never giving out CSI to visitors in the office or people on the phone

Being aware of eavesdroppers when you are talking

Never sharing information outside the office that is confidential

Keeping files locked with sensitive information

Keeping your desk clear of sensitive information except for what you are currently working with

Remember...

- You are a part of the staff and thus, you represent your department
- Talking about confidential matters outside the job is cause for dismissal
- Each department has its own procedures for making sure confidential and sensitive information is protected
- Follow the instructions of your supervisor



For More Information

FIGHTING BACK AGAINST **IDENTITY THEFT**

FEDERAL TRADE COMMISSION

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

