Red Flag

The new kid on the block

So what is a Red Flag?

In simple terms, a Red Flag is an indication or warning that a fraudulent transaction or event could be occurring as a result of identity theft.

Why is this needed?

- Identity thieves use personal identifying information to open new accounts and misuse existing accounts, credit havoc and fraud, costing consumers and businesses billions of dollars every year.

- Even though we continually put safeguards in place to prevent ID theft, criminals are becoming more sophisticated and educated every day in obtaining this information fraudulently.

- The Red Flag regulation is designed to assist in detecting when ID theft might be happening and reduce its consequences. The Federal Government requires us to comply with this regulation.

What does the FTC say we must do?

- According to the FTC, by law, we must be able to do the following:
- ***Identify*** areas of exposure of ID theft and what types of events within those areas that could be interpreted as Red Flags – what to look for
- ***Detect*** when these Red Flags indicators might be present
- ***Reduce*** the exposure of financial or personal loss to the University and to the customer who might have been a victim of ID theft by *investigating* the detected Red Flag for actual fraud and responding quickly and appropriately if fraud does indeed exist.
- ***Train*** our employees on how to accomplish all of this

Which goes back to *Why this is important.*

Appalachian Covered Accounts

The University Chancellor appointed a program administrator to evaluate the Red Flag regulations and its effect on the University. The following University Units have been identified as having potential "covered accounts":

- Student Accounts
- The AppCard Express Account
- Student Loans (currently outsourced: PERKINS)
- Student In School Payment Plans
- New River Light and Power Company
- Communication Disorders Clinic

Red Flags should be identified in each of these Units by the program administrator, which satisfies the ***Identify*** portion of the FTC regulation.

Identity thieves seek the following items:

- Address
- Telephone number
- Social Security number
- Date of Birth
- Government issued driver’s license or identification number
- Alien registration number
- Government passport number
- Employer or taxpayer identification number
- Individual identification number
- Computer’s Internet Protocol address
- Bank or other financial account routing code
- Student identification number issued by the University

So we need to pay attention to them…..

Question #1

□ **Which of the following is NOT considered Personal Identifying Information?**

A. Address

B. Phone number

C. Automobile license plate number

D. Student ID

E. Government issued driver's license number or identification number

Answer

- Answer C is correct:

  An automobile license plate number is not a government authorized form of identification. All others are recognized as valid forms of identification.

Question #2

- **Which of the following is NOT considered Personal Identifying Information by the FTC?**

A. Date of Birth

B. Social Security number

C. Employer or taxpayer identification number

D. Financial routing code

E. An individual’s height and weight

Answer

- Answer E is correct:

  Even though a person’s height and weight are personal information from an individual’s perspective, they are not considered as information to qualify as a possible Red Flag.

  All others are recognized as valid forms of identification or are protected information.

Question #3

- **Which of the following is not a Red Flag category?**

A. Notifications and warnings from credit agencies

B. Suspicious documents or personal identifying information

C. Suspicious account activity

D. Expired documents

E. Alerts and notifications from identity theft victims

Answer

- Answer D is correct:

  Expired documents do not raise Red Flags, and, in fact, expired documents can actually be utilized to verify identification.

Reduce Exposure and Limit Liability

- You need to act quickly
- First, consult your Unit's business and departmental procedures for individual departmental investigation instructions
- Gather all related information and documentation associated with the situation
- Escalate to a supervisor or manager if your investigation does not eliminate the possibility that a fraud or ID theft may be occurring
- If your investigation determines that the Red Flag is triggered by a normal and usual customer request or a general mistake, no action may be necessary –other than correcting the item in question.

Reduce Exposure and Limit Liability

- A Red Flag Incident Report should be completed if the situation can not be resolved, or if it **is** determined that a possible fraud or ID theft may be occurring

- The Incident Report will be forwarded to the Program Administrator, who is responsible for the operation of the University Red Flag Program

- If it is determined that a fraud or ID theft has actually been detected, then the owner of any compromised account MUST be notified by the Program Administrator

Who to contact?

- □ Denise Foutz, Director of Special Projects x6119

  Program Administrator

- □ Amy Roberts, Director of Special Funds x6419

- □ Julie Taubman, Director of Research Protections x7981

- □ Oscar Knight, IT Security Officer x6946