RED FLAG RULES

Appalachian State University
Identity Theft Prevention Program

Why is this important?

- The Federal Trade Commission (FTC) regulates financial transactions at Appalachian University.
- The FTC has defined Appalachian as a creditor.
- The FTC has determined that all creditors must comply with the Red Flags regulations and by law must train certain respective employees that could come in contact with a "Red Flag".

Why is this important?

- Your manager has determined that within your daily responsibilities you may come in contact with a Red Flag, and therefore need to be trained on what to look for and what to do if you see a Red Flag.

- Appalachian State University has an Identify Theft Prevention Program developed to help detect, prevent and mitigate identify theft.

Why is this important?

- This training session has a key role in this policy.
- You can access this policy in the Resource Manual under the Administration Section: Identity Theft Prevention Plan.

What will I learn?

- By completing this training module you will learn:
  - Knowledge of what is a Red Flag
  - Knowledge of what is a “covered account”
  - Knowledge of the different types of Red Flags and how they can present themselves
  - Knowledge of what to look for and where to look in detecting a Red Flag
  - Knowledge of what process to follow in case you should detect a Red Flag
  - Knowledge of whom to contact

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.*

Question #1

- What does the FTC say we must do?

A. Identify what types of indicators could be Red Flags – what to look for
B. Detect when these Red Flag indicators might be occurring
C. Mitigate or reduce the exposure not only to the University, but also to the customer who might have had his/her ID stolen
D. Train our employees on how to accomplish all of this
E. All of the above

Answer

- Answer E is correct – All of the above

The FTC requires that we be able to:

Indentify what accounts are considered "covered accounts" and what Red Flags could be present within these accounts.

Detect the Red Flags within these identified "covered accounts"

Reduce the exposure these Red Flags might cause to the University and the customer by investigating and responding appropriately

Train our employees in these areas

What is a “covered account”?

A “covered account” is a customer account that has been identified as having the possibility of a Red Flag occurrence and must be monitored for the detection of a Red Flag.

There are 2 types of covered accounts.

1. The first type deals with **individuals**. Any account that allows an individual to pay for a service or product over time with multiple payments **is** considered a covered account. An example is an extended payment schedule for tuition costs.

What is a “covered account”?

2. The second type deals with any customer account that allow **small businesses** or **individuals** to purchase products or services that are not paid in full at the time of the services or sale.

These accounts ***could be*** considered covered accounts depending upon the overall risk factors involved. As an example, this may apply to businesses that the University provides services to every month but only bills them at the end of the month.

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.

Question #2

- What is considered a "covered account"?

A. An account that allows an individual to make payments over time

B. An account for small businesses that pay for services in full at the time they are rendered

C. An account that is covered by the University in case of a student default

D. Only A and B

E. Only A

F. All of the above

Answer

Only A is correct

- For individuals, covered accounts include any account that allows individuals to make multiple payments to pay off an obligation.

- Only small business accounts or individuals that do not pay at the time the product or service is received (such as monthly billing) could be considered as "covered" by the Red Flag Regulation. These may or may not be considered as covered based upon the risk associated with identity theft. These accounts have been determined by the University Red Flag Rules Program Administrator.

Question #3

- **Is cashing a check for a student considered a "covered account activity" ?**

- A. Yes

- B. No

Answer

- Answer: No, but remember ….we do not cash checks on campus.
- Single transaction items, such as cashing a check for a student, are not considered as covered account activities by the regulation.
- Also, purchasing a book or article from the bookstore or cafeteria on your credit card is not considered as "covered" by the Red Flag Rules.
- For individuals, accounts or transactions that allow the individual to make multiple payments over time are considered as "covered".
- **NOTE: Even though these types of transactions are not covered under the Red Flag regulations, there may be other University policies, procedures, and guidelines that must be followed when dealing with them.**

Identity thieves may steal 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…..

What should you look for?

- A Red Flag may indicate that identity theft has occurred and fraud could be in progress.
- Red Flags come in 5 categories (flavors)……
- •Notifications and Warnings from Consumer Reporting Agencies
- •Suspicious Documents
- •Suspicious Personal Identifying Information
- •Suspicious Covered Account Activity
- •Alerts from Others

Question #4

- **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 #5

- **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 #6

- **Which of the following is <u>not</u> 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.

Red Flag Program – General Training

- Topics to be covered in this section include:

- Examples of the 5 categories of Red Flags:
  - •Notifications and Warnings from Consumer Credit Bureaus
  - •Suspicious Documents
  - •Suspicious Personal Identifying Information
  - •Suspicious Covered Account Activity
  - •Alerts from Others

- Where Can Red Flags Be Detected
- How to Detect Red Flags
- Reduce Exposure and Liability
- General Correspondence
- Third Party Contracts
- Updates to the Red Flag Program

General Training
Notification from Consumer Credit Bureaus

- Examples:

- A fraud alert has been included with a consumer credit report from a credit bureau

- A notice of a credit freeze has been provided in response to a request for a consumer credit report from a credit bureau

- A consumer credit bureau provides a notice of address discrepancy

- A consumer credit bureau reports unusual credit activity, such as an increased number of accounts or inquiries

General Training
Suspicious Documents

- **Examples:**

- Documents provided for identification that appear to be altered or forged

- Photograph on ID does not match the appearance of the individual or does not look like the individual

- Information on ID does not match the information provided by the person opening the account

- Application appearing forged, altered, or destroyed and reassembled

General Training
Suspicious Personal Indentifying Information

- <u>Examples:</u>

- Information on an ID does not match any address in the consumer report

- The Social Security number has not been issued or appears on the Social Security Administration's Death Master File (a file of information associated with Social Security numbers of those who are deceased)

- There is a lack of correlation between the Social Security number provided and the range for the date of birth

- Personal identifying information that is provided is associated with known fraud activity

General Training
Suspicious Personal Indentifying Information

- Examples(cont.)

- A suspicious address is supplied, such as a mail drop or prison

- A phone number associated with pagers or answering service is given

- A duplicate Social Security number is provided that matches one submitted by another person opening an account or another customer with an existing account

- Duplicate addresses or phone numbers that match others are supplied by a large number of applicants

General Training
Suspicious Personal Indentifying Information

- Examples (cont.)

- The person opening the account is unable to supply identifying information when told that the application is incomplete

- The applicant's personal information is inconsistent with information already on file

- The person opening an account or an existing customer is unable to correctly answer challenge questions

General Training
Suspicious Covered Account Activity

- <u>Examples:</u>

- Shortly after a change of address on an account, you receive a request for additional users of the account

- You notice that most of the available credit for an account is used for cash advances, jewelry or electronics, plus the customer fails to make the first payment

- You notice a drastic change in payment patterns, use of available credit, or spending patterns on an account

- You notice that an account that has been inactive for a long time suddenly has lots of unusual activity

General Training
Suspicious Covered Account Activity

- Examples (cont.)

- You notice that mail that has been sent to a customer is repeatedly returned as undeliverable despite transactions continuing to occur on the account

- You are notified that a customer is not receiving his/her account statements

- You are notified of unauthorized charges or transactions on a customer's account

General Training
Alerts from Others

- Examples:

- You receive some notification from a third party (such as law enforcement, an attorney, a credit bureau) that there is a fraudulent account being used at the University by a person engaged in identity theft

General Training
Where can Red Flags be detected?

- The opening of a customer account, such as a student loan, the activation of a new AppCard, or a utility account
- The ongoing monitoring of one of these customer accounts for suspicious activities
- General correspondence with a customer -written or verbal
- Information received from Credit Agencies or Credit Bureaus that might lead you to be suspicious that there **could be** an identity theft problem

General Training
How to Detect Red Flags

- <u>Examples:</u>
- Verify identities when opening customer accounts or performing customer transactions
- Monitor ongoing transactions of customer accounts, such as Appcard transactions
- Verify the validity of any change to address or bank routing information or other relevant information to a customer account
- •Watch for credit bureau report warnings
- **•Be aware –identity fraud is all around us**

Question #7

- **Where can Red Flags be detected?**

A. The opening of a customer account

B. The ongoing monitoring of a customer account

C. A response from a credit bureau

D. Both A and B

E. All of the above

Anwer

- Answer E is correct: All of the Above

- Red flags can be detected when opening a new covered account, while monitoring an existing covered account, in general communications or correspondence with a customer, and with notifications from a credit bureau.

- Looking for suspicious documents and mismatching IDs should be accomplished when opening new accounts.

- Existing accounts should be monitored for unusual activity and notifications from customers concerning invalid or unauthorized transactions.

- Also, all correspondence from a credit bureau or agency should be monitored for possible signals for ID theft or Red Flags.

Question #8

- **Are all Customer Accounts considered as Covered Accounts**

A. Yes

B. No

Answer

- Answer B is correct: No

- Not all customer accounts are necessarily considered as covered accounts under the Red Flag regulations.

- Any individual account that offers multiple payments over time is always considered a covered account.

- Other customer accounts (both small business and individual accounts) that allow the purchase of a service or product without the immediate payment by the customer could be considered a covered account, based on the financial and personal risks to both the customer and the University. If there is limited risk involved, then the customer account does not require designation as a covered account.

General Training
Reduce Exposure and Liablity

- 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.

General Training
Reduce Exposure and Liability

- The Supervisor will complete a Red Flag Incident Report 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

General Training
Reduce Exposure and Liability

- Subsequent actions by the Program Administrator may include:

- Notifying in writing the original customer/vendor/supplier/student of all ongoing investigations and outcomes

- Notifying proper government or law enforcement entities and utilizing such for an ongoing investigation

- Taking all actions required by law in handling a fraudulent account as defined by the FTC, the University, and any local, state, or federal laws

- Maintain all incident reports and pertinent information for reporting purposes and future references

Question #9

- **Which of the following is <u>NOT</u> part of the process for Reducing Exposure and Liability?**

A. You must act quickly

B. You must follow all individual department procedures and regulations

C. You must gather all information and documentation

D. For every Red Flag identified, you must complete the Red Flag Incident Report and forward it to the Program Administrator

E. None of the above

Answer

- Answer D is correct:

- The Program Administrator should not be notified unless there has been a potential fraud determined through investigation, not just if a Red Flag has been detected. A thorough investigation needs to be completed by the individual and his/her management prior to involving the Program Administrator.

- The other items listed should occur during the process. Gather all information, follow internal department processes, and remember to act quickly because, if it is an actual fraud, speed is of the essence in determining this and stopping any future fraudulent activities.

General Correspondence

- All correspondence, written or verbal, both to and from a customer, vendor, or supplier, could indicate a Red Flag and possible ID fraud. The following are examples of such correspondence:

- Mail sent to a customer/vendor/supplier is repeatedly returned as undeliverable despite ongoing transactions on an active account.
- You are notified that a customer/vendor/supplier is not receiving account statements or payments.
- You are notified of unauthorized charges, transactions, or modifications on customer/vendor/supplier accounts.
- You are notified that a fraudulent account for a person engaged in identity theft has been opened at the University.

Third Party Contracts

- All managers/supervisors must exercise appropriate and effective oversight of service provider or third party arrangements.

- There are certain service providers who may be the only ones that are able to detect Red Flags. Examples are debt collectors that may be hired to contact customers for outstanding debts. Another example could be an agency that collects payments for the University. These types of service providers must have a defined and implemented Red Flag Program and must certify as such to the University via the contract agreement.

- Examples within the University of such service providers include, but are not limited to:

- ECSI –Educational Computer Systems, Inc. (Student Loan Management)
- Sallie Mae –Tuition Payment Plans
- Other Collection Agencies that provide collection services for Student Accounts
- Other Federal & State Agencies that provide payments on accounts for Students???

Updates to the Red Flag Program

- The University has assessed various Units and has identified Units that contain covered accounts and defined Red Flags within these accounts.

- If you believe that there are other accounts that could qualify as covered accounts and should be included in the Red Flag Program, please contact the Program Administrator. Contact information is located within the Contact and References section of this training module.

Congratulations

- You have now completed the section on Red Flag training for **General Training**

References and Contacts

Contact Information:

- For further information, questions, or updates to the Red Flag Program contact Denise Foutz, foutzdn@appstate.edu

References and Forms:

- Appalachian State University Identity Theft Prevention Program – Resource Manual
- FTC 16 CFR Part 313 – Gramm-Leach Bliley Act – Privacy
- FTC 16 CFR Part 314 – Gramm-Leach Bliley Act – Safe Guarding Customer Information
- Appalachian State University Identity Theft Prevention Program Procedural Guide
- Red Flag Incident Report Form