Why Should UNC Asheville be Concerned?

• The Federal Trade Commission (FTC) regulates financial transactions at UNC Asheville

• The FTC has defined UNC Asheville as a creditor.

• The FTC has determined that all creditors must comply with the Red Flags regulation and by law must train certain respective employees that could come in contact with a “Red Flag”.
What Should I 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
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 Information Important?

Identity thieves use personal identifying information to open new accounts and misuse existing accounts, creating 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 (Federal Trade Commission) Require?

According to the FTC, by law, we must be able to do the following:

- Identify areas of exposure to ID theft and what types of events within those areas could be interpreted as Red Flags (i.e. what to look for)
- Detect when these Red Flag 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 Flags for actual fraud and responding quickly and appropriately if fraud does indeed exist
- Train our employees on how to accomplish all of this
How Is It All Related?

- UNC Asheville must identify “Covered Accounts” as outlined in the FTC’s Red Flag Rule.
- UNC Asheville must implement a written Identity Theft Prevention Program designed to detect the warning signs — or "red flags" — of identity theft in their day-to-day operations.
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.

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.*

The second type deals with any customer account that allows small businesses or individuals to purchase products or services that are not paid in full at the time of the service or sale. These accounts could be considered covered accounts, depending upon the overall risk factors involved.
UNC Asheville Covered Accounts

The following are possible university “covered accounts”:

• Student Accounts
• The Campus OneCard
• Short Term Student Loans
What Types of Data Do Identity Thieves Want?

- 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.....
How Should We Be on the Lookout?

Red Flags may indicate that identity theft has occurred and fraud could be in progress.

Red Flags come in 5 CATEGORIES

• NOTIFICATIONS AND WARNINGS FROM CONSUMER REPORTING AGENCIES
• SUSPICIOUS DOCUMENTS
• SUSPICIOUS PERSONAL IDENTIFYING INFORMATION
• SUSPICIOUS COVERED ACCOUNT ACTIVITY
• ALERTS FROM OTHERS
Notifications and Warnings from Consumer Reporting Agencies

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
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
Suspicious Personal Identifying Information

Examples:

- 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
More Suspicious Personal Identifying Information

More Examples:

• A suspicious address is supplied, such as a mail drop or prison
• 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
More Suspicious Personal Identifying Information

General Examples:

• 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
Suspicious Covered Account Activity

Examples:

• Shortly after a change of address on an account, you receive a request for additional users of the account
• 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
More Suspicious Covered Account Activity

More Examples:

• 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
Alerts from Others

Example:

• 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
Where Can Red Flags be Detected?

• The opening of a customer account, such as a student long term or short term loan, or the activation of a new OneCard

• 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
Detection From 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.
Risks of 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 may include, but are not limited to:

- Student Loan Management
- Extended Tuition Payment Services
- Credit Checks
How Can I Help Detect Red Flags?

• Verify identities when opening customer accounts or performing customer transactions

• Monitor ongoing transactions of customer accounts, such as OneCard 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
What Should I Do?

• You need to act quickly
• First, consult your University business and departmental procedures for individual departmental instructions or guidance
• 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.
What Happens Next?

• You or your Supervisor report the potential issue using an e-mail to redflag@unca.edu if the situation cannot be resolved, or if it is determined that a possible fraud or ID theft may be occurring

• The issue will be reviewed by the Program Administrator, who is responsible for the operation of the University Red Flag Program

• Others on the Red Flag Committee or Technical Experts will be consulted as needed

• 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
And Then?

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
• Maintaining all incident reports and pertinent information for reporting purposes and future references
Help Us Protect Identity

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 or any member of the Red Flag Rules Committee. Contact information is located within the Contact and References section of this training module.
Contacts

UNC Asheville Identity Theft Prevention Program Red Flag Committee

Suzanne Bryson – AVC Finance, Program Administrator
Karen Shaw – Controller
Jeff Brown – Chief Information Officer
Adam Reagan – Associate Chief Information Officer

Monique Taylor – Internal Audit Director (Advisory Capacity)
References

UNC Asheville Identity Theft Prevention Program
(http://finance.unca.edu/sites/finance.unca.edu/files/Finance/UNC_Asheville_Red_Flags_Program.pdf)

NC Identity Theft Prevention Act
(http://www.ncleg.net/EnactedLegislation/Statutes/PDF/ByArticle/Chapter_75/Article_2A.pdf)

FTC Red Flag General Information
(http://www.ftc.gov/bcp/edu/microsites/redflagsrule/index.shtml)

FTC 16 CFR Part 313 -Gramm-Leach-Bliley Act -Privacy
(http://www.ftc.gov/os/2000/05/65fr33645.pdf)

FTC 16 CFR Part 314 -Gramm-Leach-Bliley Act –Safeguarding Customer Information
(http://www.ftc.gov/os/2002/05/67fr36585.pdf)

FTC 16 CFR Part 681 -Identity Theft Rules