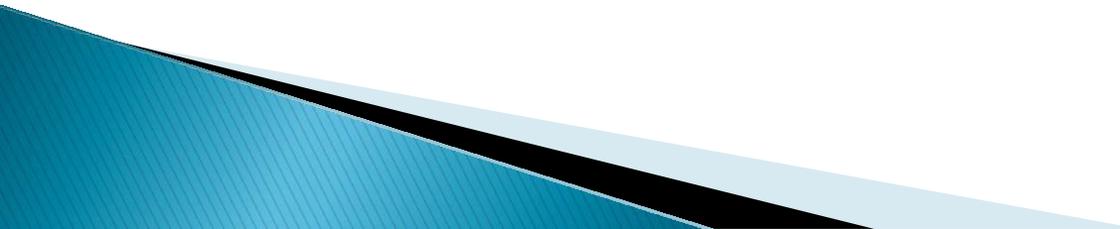


Red Flag Training

Detecting, Preventing and Mitigating Identity Theft

Presented by the Bursar's Office

Goals of Training

- ▶ To explain the federal rules intended to prevent Identity Theft and how they apply to the University,
 - ▶ To identify risks that alert you to a potential fraudulent activity,
 - ▶ To assist you in detecting when these risks occur on a student's account, and
 - ▶ To review how you should respond once you've detected a potential fraudulent activity.
- 

What is Identity Theft?

A fraud committed or attempted using the identifying information of another person without authority.



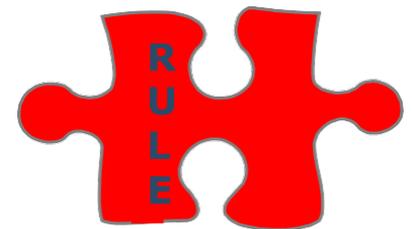
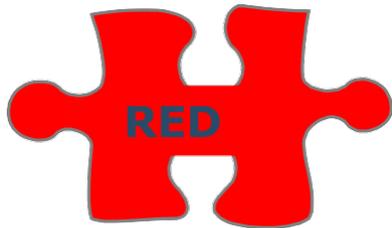
What is a **Red Flag**?

A pattern, practice, or specific activity that indicates the possible existence of identity theft.



What is Red Flags Rule ?

- ▶ In November 2007, final rules were issued to implement the *Identity Theft Red Flags Rule*.
- ▶ The Rule applies to financial institutions and creditors that offer or maintain accounts.
- ▶ The Rule requires the implementation of a written Identity Theft Prevention Program. All procedures must be fully implemented by June 2010!



Why does this apply to SIUE?

Under the law, you are a **creditor** if you sell customer services now and bill them later.

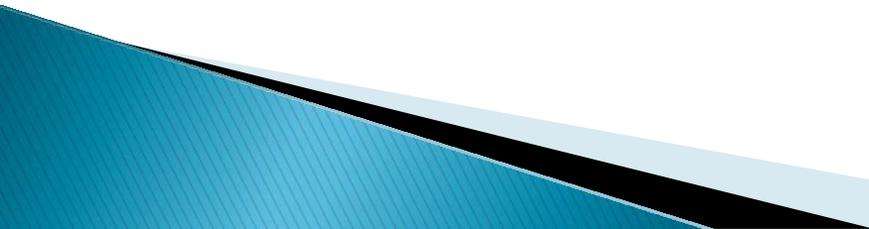
The Installment Payment Plan offered to students makes SIUE a creditor and subject to the Red Flags Rule. Financial aid like short term loans and Perkins loans are also creditor activities that SIUE administers.

Why isn't it just a Bursar's Office problem?

- ▶ Offices throughout campus access and update customer records.
- ▶ Red Flags Rule is about protecting customer records in order to *prevent, detect* and *mitigate* identity theft.

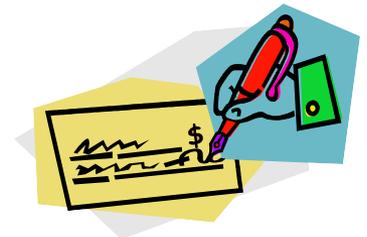


Covered Accounts

- ▶ The Rule's goal is to detect, prevent, and mitigate identity theft in certain *covered accounts*.
 - ▶ A covered account is a continuing relationship established to provide a financial product or service and includes all consumer accounts or loans that are administered by the University.
 - ▶ Student account information on **Banner** and **CougarNet** are “covered accounts”.
- 

New and existing **covered accounts**...

- ▶ Risks may arise when updating accounts already established in Banner and CougarNet.
- ▶ Risks may arise when creating new accounts.
- ▶ How are new accounts created?
 - When apply for admission to the University
 - When apply for campus housing
 - When a service is rendered and billed for later
 - When fines are imposed (parking, library, etc.)
 - When apply for financial aid and loans



Identifying Red Flags

A Red Flag, or any situation closely resembling one, should be investigated for verification. The following are potential indicators of fraud:

- ▶ Identification document or ID card that appears to be forged, altered or inauthentic;
- ▶ Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the identification;
- ▶ Other information on the identification is not consistent with existing student information;



More Red Flags...

- ▶ Application for service that appears to have been altered or forged;
- ▶ Social security number presented that is the same as one given by another student;
- ▶ A person fails to provide complete personal identifying information on an application when reminded to do so;



More Red Flags...

- ▶ A person's identifying information is not consistent with the information that is on file for the student;
- ▶ A person's identifying information provided is inconsistent when compared against external information sources;



More Red Flags...

- ▶ University is notified that the University has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.
- ▶ This notice may come from...
 - a student,
 - an Identity Theft victim,
 - law enforcement, or
 - other person.



Examples of **Suspicious** Personal Information

The address does not match any address on record;

The address on a document is the same as the address provided on a known fraudulent document;

The address on a document is fictitious, a mail drop, or a prison; and

The phone number is invalid or is associated with a pager or answering service.





Just how suspicious...?

...a SSN provided for an account is the same as one provided by another person for a different account?

How would you know?

...the person opening a Covered Account fails to provide all the required personal identifying information on an application and then doesn't respond to notices that the application is incomplete?

What do you do next?

...a person requesting access to a Covered Account cannot answer the security questions (mother's maiden name, pet's name, etc.)?

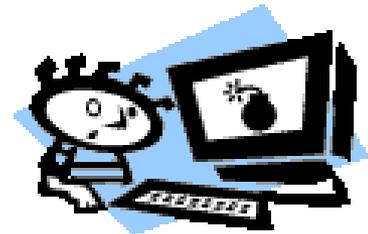
How do you handle this?



Sometimes it's not that obvious...

Do you know what to do if...

- ▶ ...mail sent to the account-holder is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the Student Account?
- ▶ ...the University is notified that a customer is not receiving documents, even though they were mailed and not returned?



Sometimes it is that obvious...

- ▶ Do you know what to do when...
 - ...the University receives a notice regarding possible identity theft in connection with a student???
 - ...the University is notified that your department has opened a fraudulent account for a student engaged in identity theft???



Stay alert for **red flags**...

- ▶ What red flags might you detect in your department?
- ▶ Do you know what to do if you suspect something fraudulent?
- ▶ How can you best protect your customers?



Responding to Red Flags

- ▶ Report known and suspected fraudulent activity immediately to your supervisor.
- ▶ Gather information and documentation on the activity;
- ▶ Continue to monitor a Covered Account for evidence of Identity Theft.
- ▶ Notify the student that you suspect Identity Theft involving their University account.
- ▶ Change any passwords or other security devices that permit access to the accounts
- ▶ Notify Campus Police.
- ▶ Inform the Bursar's Office.



It's all about **security**...

- Store restricted information on secure servers, **never on your workstation.**
- Password protect your computer and set your screensaver to come on automatically.
- Do not send restricted information via email.
- Cross-shred all restricted data documents before throwing them away.
- Keep conversations quiet, make sure they cannot be overheard when exchanging restricted data.



Want to learn more?

Visit the **Red Flags Website**:

The Federal Trade Commission's information page.

<http://www.ftc.gov/redflagsrule>

Thank you!

Questions? Contact the Bursar's Office

Dawn Sparks dsparks@siue.edu or

James Burgdorf jburgdo@siue.edu.