



# **RED FLAG RULES: IDENTITY THEFT PROTECTION**

**Lamar State College – Port Arthur**



# Objective

## **Participants will:**

- Understanding Red Flag Rules
- Understanding why Red Flags are important on our campus
- Identifying Red Flag Rules
- Complying with Red Flag Rules
- Detecting Red Flag Rules
- Preventing and Mitigating Identity Theft On Campus
- Updating the LSCPA Red Flag Rules Program
- Additional Red Flag Rules Resources

# LSCPA Red Flag Rules Program Oversight Team

## (referenced throughout this presentation)

- **Program Administrator:**
  - Director of Cash Management - Karen Snyder
- **Program Coordinators:**
  - VP for Student Services - Tom Neal
  - Director of Financial Aid - Diane Hargett
  - VP for Finance – Gwen Reck
  - Registrar – Connie Nicholas
  - Director of Human Resources Linda McGee
  - Chief Information Officer – Samir Ghorayeb



# Red Flags Rules Defined

- A “**RED FLAG**” is defined as “a pattern, practice or specific activity involving a college community member (faculty, staff, or student) that indicates the possible existence of identity theft”
- Purpose of this training is to help you better identify the warning signs or “**red flags**” of identity theft in the day-to-day operations of the college and campus operations
- Enables financial institutions to detect and defend students against fraud and identity theft

# Definitions

- **Creditor** – an entity which defers payment for services rendered, such as an organization that bills at the end of the month for services rendered the previous month.
- **Covered Account** – a customer account that involves multiple payments, transactions or any other account for which there is a reasonably foreseeable risk for identity theft.
- **Financial Institution** – defined as a state or national bank, a state or federal savings and loan association, a mutual savings bank, a state or federal credit union, or any other entity that holds a “transaction account” belonging to a consumer.
- **Transaction account** – a deposit or other account from which the owner makes payments or transfers.
- **Identity Theft** – Fraud committed or attempted using the identifying information of another person without authorization.



# Covered Accounts at LSCPA

- Student Accounts
- Student Loans
- Deferment of Tuition Payments
- Emergency Loans

# Rules Governing Red Flags Rules

- Rules are designed to align with mandate issued by the Federal Government
  - Sections 114 and 315 of Fair and Accurate Credit Transactions Act of 2003
  - FTC, Federal Financial Institution Regulatory Agencies, and National Credit Union adopted these regulations in October 2007
  - Became known as **Red Flags** Rule





# The Facts

- In 2008, there were 10 million victims of identity theft in the United States. This presented a 22% increase over 2007.
  - (Javelin Strategy and Research, 2009)
- In the United States, 1 in every 10 consumers has already been victimized by identity theft.
  - (Javelin Strategy and Research, 2009)
- 38-48% of victims discover their identity has been compromised within three months, while 9-18% of victims do not learn that their identity has been stolen for 4 or more years.
  - (Identity Theft Resource Center Aftermath Study, 2004)

# College Students are the #1 Target

- 31% of identity theft victims fall between the ages of 18-29.
  - (Federal Trade Commission)

## Top 3 Reasons according to Dave Ramsey

1. Naivety
2. Receive many credit card offers
3. Failure to examine financial records



# The Aftermath

- On average, victims lose between \$851 and \$1,378 out-of-pocket trying to resolve identity theft.
  - (ITRC Aftermath Study, 2004)
- 70% of victims have difficulty removing negative information that resulted from identity theft from their credit report.
  - (ITRC Aftermath Study, 2004)
- 47% of victims encounter problems qualifying for a new loan.
  - (ITRC Aftermath Study, 2004)



# Identifying Risks

- LSCPA must regard any threat of identity theft as an immediate and highly important matter
- Steps should be taken and enforced immediately to mitigate fraud
  - **Detect**
  - **Deter**
  - **Defend**





# Costs to College

**Identity theft not only costs our students heartache, time, and money-----it impacts the campus.**

- **Stolen Services**
- **Loss of Personnel Time**

# Red Flag Rules

- Red Flag Rule requires creditors (i.e. LSCPA) to offer/maintain covered accounts to adopt a written identity theft prevention program and train its employees how to:
- Detect warning signs of identity theft in day to day campus operations
- Take Steps to Prevent identity theft on campus
- Mitigate any damage or liability to the students



# Red Flag Rules

- LSCPA campus administrators are most likely to detect Red Flags during:
  - **Admissions Process**
  - **Applying for Financial Aid**
  - **During set-up of an Installment or Short Term Loan**



# Steps to Compliance

In order to comply with the Federal Red Flags Rule, LSCPA had to:

1. Conduct a Risk Assessment and identify Potential Red Flag Areas for our campus
2. Set up procedures for detecting Red Flags
3. Respond to Red Flags instances immediately to prevent theft/mitigate damages
4. Train our employees/front line staff on Red Flag program and detection procedures



# Prevention: Identify Red Flags


Categories of Red Flags on our Campus are:

1. Presentation of suspicious documents
2. Presentation of suspicious personal identifying information
3. Suspicious account activity
4. Notice from External/Other Sources



# How To Recognize Suspicious Documents

- Documents appear to have been:
  - Altered or forged
  - Give the appearance of having been destroyed and reassembled
- The person presenting the identification does not look like the photograph or match the physical description
  - Weight
  - Hair Color
  - Age



# How To Recognize Suspicious Documents & Personal Identifying Information (PII)

- Information on the ID differs from what the person is telling you
- Identifying Information on the ID is not consistent with readily accessible information in LSCPA system.
  - Address
  - Birth date



# Suspicious Personal Identifying Information

“Identifying Information” means “any name or number that can be used, alone or in conjunction with any other information, to identify a specific person.”

## Includes:

- Name
- Social Security Number
- State or Gov. Issued ID Number
- Alien Registration Number
- Government Passport Number
- Employer or Taxpayer Identification Number
- Electronic ID Number (e.g. banking routing code)



# Suspicious Personal Identifying Information

- PII provided is a type commonly associated with fraudulent activity
  - Address is fictitious
  - Phone number is invalid <e.g. (123) 456-7890>
  - Phone number is pager or answering services
- SSN matches another student on file
- SSN is invalid
  - First three digits are in the 800, 900, or 000 range
  - In the 700 range above 772, or are 666
  - The fourth and fifth digits are 00
  - The last four digits are 0000



# Suspicious Personal Identifying Information

- Student on the covered account (or student account) does not provide all the required PII during registration
- Student does not respond to registration being incomplete
- Signatures on paperwork is not consistent
- Student cannot provide authenticating information or answer to challenge question beyond which is general information that could be readily accessible
  - **Wallet, Consumer report, Facebook**

# Suspicious Account Activity

- Mail sent to student is returned repeatedly as undeliverable
  - Even though transactions or correspondence continues to come from that student address
- College is notified of unauthorized transactions in connection with a student's account
- The student account shows unusual activities, inconsistent with established patterns
  - Non-payment when there is no history of this before

# Notice from External Sources

- College receives notice from:
  - Student
  - Victims of Identity Theft
  - Law Enforcement Authorities
  - Other External Agency (e.g. credit bureau, etc)
- Student disputes a bill/student registration charge by claiming to be the victim of identity theft



# Detection of Red Flags

- College administrators should exercise due diligence in the detection of **Red Flags** by:
  - Asking for and verifying identification before answering questions or rendering services
  - Being alert for Red Flags in day to day operations



# Detection of Red Flags

- If students ask the reason for your identification procedures, administrators should simply explain that the procedures are for “privacy reasons and to protect students’ security”



# Prevent & Mitigate Identity Theft

- Notify your Supervisor/Department Head any time you:
  - **Encounter Suspicious documents**
  - **Encounter Suspicious Personal Identifying Information**
  - **Suspicious Account Activity**
  - **Receive notice of Red Flags or identify theft from other sources**





# Prevent & Mitigate Identity Theft

- If you receive a phone call from a student about a possible identity theft case or discrepancy:
  - Request the student supply a written report to one of the Program Coordinators at the College
  - Advise student to report the identity theft to local police and provide any one of the Program Coordinators with a copy of the police report
  - Advise student to change any and all computer passwords, security codes, and other permit access to covered accounts and/or other related financial accounts
  - Retain copies of Documentation included with the report
  - Note the discrepancy on student account or in their file so that others are aware when the student's information is retrieved.



# Proactive Measures-Program Oversight

- LSCPA Red Flag Program will have ground level monitoring by Program Coordinators
- ANY noted potential identity theft issues should be reported Immediately to one of the Program Coordinators
- Program Coordinator will report to Program Administrator



# Proactive Measures-Program Oversight

- Program Coordinators should:
  - Maintain a log of incidents in their area
  - Immediately report incidents to Program Administrator for further investigation
  - Take responsibility for ensuring availability and compliance of departmental training
  - Provide, on a semi-annual basis, the Program Administrator with suggested Red Flag Program updates to reflect changes in risk assessment to students



# Proactive Measures-Program Oversight

- Program Administrator will:
  - Forward any necessary case to the Program Coordinator for that area who will work with Student Services to contact Law enforcement for investigation
  - Recommend to or Approve Student Services to issue a new Student ID, when warranted
  - Report any warranted cases to third party agencies
  - Recommend additional training as warranted

# Reponses to Red Flag Reports

After receiving a report, possible responses include:

- Re-opening a covered account with a new account number and/or LSCPA student ID
- Not attempting to collect on a covered account or not selling a covered account under question to Retail Merchants for collection
- Program Administrator will report instance(s) to:
  - Other campus administrators
  - Law enforcement
  - Credit Bureaus

# Reponses to Red Flag Reports

- Determining no response is warranted under particular circumstances by Departmental Program Coordinator
  - No evidence of Identity Theft is Determined
- Placing the covered account “on hold” from any further access, use, or disclosure until the Red Flag event is fully investigated by authorities
- Isolating and correcting inaccuracies in student records resulting from identity theft with the Program Coordinator for that area



# Conclusion

- It is anticipated that most cases and subsequent investigation of detected Red Flags will be discovered and will remain at the Departmental Level. However, on the part of due diligence, all instances will be investigated and confirmed by the Program Coordinator for that area working with the Program Administrator.
- Where there is a strong indication of identity theft, the Departmental Red Flag Program Coordinator will fill out a Red Flag Incident Report and send it immediately to the Program Administrator.

# Review

- Take reasonable measures to control foreseeable risks
- Identify Risk Factors and sources of Red Flags
- Detect any Red Flags through identifying information



# Review

- Establish proactive measures to reduce Identity Theft
- Update policy as new Identity Theft risks emerge





## References & Additional Resources

- Federal Register, Part IV, Federal Trade Commission 16 CFR Part 681.
- Federal Trade Commission. Retrieved from <http://www.ftc.gov/redflagsrule>
- NACUBO. Retrieved from [http://www.nacubo.org/Initiatives/FTC\\_Red\\_Flags\\_Rule.html](http://www.nacubo.org/Initiatives/FTC_Red_Flags_Rule.html)



**QUESTIONS?**





# *Certificate of Completion*

*I certify and attest that I have read and completed the on-line training course*

*RED FLAGS RULE:*

*IDENTITY THEFT PROTECTION*

*Name: \_\_\_\_\_*

*Signature: \_\_\_\_\_*

*Title: \_\_\_\_\_*

*Department: \_\_\_\_\_*

*Date: \_\_\_\_\_*

*Lamar State College – Port Arthur*

*A Member of The Texas State University System*