Information Security:
Identity Theft Protection and Red Flag Rules

Technology Services

1/6/2012

LAMAR INSTITUTE OF TECHNOLOGY
TECHNOLOGY SERVICES

Identity Theft Protection

The purpose of this session is to:

- Establish a Red Flag Rules Program
- Communicate why Red Flags are important on our campus
- Insure compliance with Red Flag Rules
- Demonstrate how to detect Red Flags
- Demonstrate how to prevent and Mitigate Identity Theft On Campus

LAMAR INSTITUTE OF TECHNOLOGY
TECHNOLOGY SERVICES

Red Flags Rules Defined

- A “RED FLAG” is defined as “a pattern, practice or specific activity involving an LIT 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 an LIT 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 or transactions. The establishment of a "continuing relationship" with the institution is also advised.

Definitions (Cont.)

- 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.

LAMAR INSTITUTE OF TECHNOLOGY
TECHNOLOGY SERVICES

Covered Accounts at LIT

- Student Accounts
- Student Loans
- Deferment of Tuition Payments
- Emergency Loans
- LIT Health Center Patients
- Dental Hygiene Patients

Rules Governing Red Flags Rules

Rules aligned with Federal Mandate

- 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)

The Facts (Cont.)

- 38-48% 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)

The ITRC Aftermath Study, 2004

Identity Theft Resource Center

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

Identifying Risks

- LIT 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 LIT

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

- Stolen Services
- Loss of Personnel Time

LAMAR INSTITUTE OF TECHNOLOGY
TECHNOLOGY SERVICES

Red Flag Rules

Red Flag Rule requires creditors (i.e. LIT) 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

Red Flag Rules (Cont.)

- Mitigate any damage or liability to the students
- LIT campus administrators are most likely to detect Red Flags during:
  - Admissions Process
  - Applying for Financial Aid
  - Point of Sale Process

LAMAR INSTITUTE OF TECHNOLOGY
TECHNOLOGY SERVICES

Steps to Compliance

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

- Conduct a Risk Assessment and identify Potential Red Flag Areas for our campus
- Set up procedures for detecting Red Flags
- Respond to Red Flags instances immediately to prevent theft/mitigate damages
- Train our employees/front line staff on Red Flag program and how to detect

LAMAR INSTITUTE OF TECHNOLOGY
TECHNOLOGY SERVICES

Identifying Red Flags

Categories of Red Flags on our Campus are:

- Presentation of suspicious documents
- Presentation of suspicious personal identifying information
- Suspicious account activity
- Notice from External/Other Sources

Identifying Red Flags (Cont.)

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

Identifying Red Flags (Cont.)

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 Banner.
  - Address
  - Birthdate

Identifying Red Flags (Cont.)

Suspicious Personal Identifying Information (PII)

"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

Identifying Red Flags (Cont.)

"Identifying Information" (Cont.)

- Government Passport Number
- Employer or Taxpayer Identification Number
- Electronic ID Number (e.g. banking routing code)
- 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

Identifying Red Flags (Cont.)

"Identifying Information" (Cont.)

- 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
- Student on the covered account (or student account) does not provide all the required PII during registration

Identifying Red Flags (Cont.)

"Identifying Information" (Cont.)

- 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

Identifying Red Flags (Cont.)

Suspicious Account Activity

- Mail sent to student is returned repeatedly as undeliverable
  - Even though transactions or correspondence continues to come from that student address
- LIT 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

Identifying Red Flags (Cont.)

Notice from External Sources

- LIT 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

LAMAR INSTITUTE OF TECHNOLOGY
TECHNOLOGY SERVICES

Detection of Red Flags

- LIT 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

- 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”

LAMAR INSTITUTE OF TECHNOLOGY
TECHNOLOGY SERVICES

Prevent & Mitigate Identity Theft

Notify your Supervisor/Department Head any time you:

- Encounter Suspicious documents
- Encounter Suspicious Personal identifying Info
- Suspicious Account Activity
- Receive notice of Red Flags or identify theft from other sources

Prevent & Mitigate Identity Theft (Cont.)

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 the Department
- Advise student to report the identity theft to local/campus police and provide LIT with copy of 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

Prevent & Mitigate Identity Theft (Cont.)

If you receive a phone call from a student about a possible identity theft case or discrepancy: (Cont.)

- 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.

LAMAR INSTITUTE OF TECHNOLOGY
TECHNOLOGY SERVICES

Red Flag Rules - Program Oversight

- LIT 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

LAMAR INSTITUTE OF TECHNOLOGY
TECHNOLOGY SERVICES

LIT Program Oversight Team

Program Administrator:

- VP for Finance & Operations

Program Coordinators:

- Finance Office
- Student Services Office
- Financial Aid Office
- Bursar's Office
- Technology Services Office

LIT Program Oversight Team (Cont.)

Program Administrator will:

- Forward any necessary case to appropriate authorities for investigation
- Recommend to or Approve Technology Services to issue a new user ID for a student, when warranted
- Report any warranted cases to third party agencies
- Recommend additional training as warranted

LIT Program Oversight Team (Cont.)

Program Coordinators should:

- Maintain a log of incidents in their area
- Immediately report incidents to Program Administrator for further investigation
- Responsible 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

Reponses to Red Flag Reports

After receiving a report, possible responses include:

- Re-opening a covered account with a new account number/student ID
- Not attempting to collect on a covered account or not selling a covered account under question

Program Coordinators will report instance(s) to:

- Other campus administrators
- Law enforcement
- Credit Bureaus

Reponses to Red Flag Reports (Cont.)

- 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

Conclusion

- It's anticipated that most cases and subsequent investigation of detected Red Flags will be discovered and will remain at the Departmental Level

- Where there is a strong indication of identity theft, the Departmental Red Flag Program Coordinator will notify the Program Administrator

LAMAR INSTITUTE OF TECHNOLOGY
TECHNOLOGY SERVICES

Review

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