Identity Theft Policy

Created: June 10, 2009 | Updated: May 5, 2016
Author: Financial Services and Information Technology Services
Version: 1.1

Scope:

The risk to Loyola University Chicago and its faculty, staff and students from data loss and identity theft is of significant concern. All members of the University community and third party affiliates share in the responsibility of reducing this risk and protecting information for which they have access of custodianship.

Purpose:

The University adopts this policy to help protect faculty, staff, students and the University from damages related to the loss or misuse of Loyola Protected and Loyola Sensitive information as defined by the University's **Data Classification Policy**.

This policy will place the University in compliance with state and federal law regarding identity theft protection, specifically the federal Red Flag Rule.

This policy will help the University:

1. Identify risks that signify potentially fraudulent activity within new or existing covered accounts;
2. Detect risks when they occur in covered accounts;
3. Respond to risks to determine if fraudulent activity has occurred and act if fraud has been attempted or committed; and
4. Update the program periodically, including reviewing the accounts that are covered and the identified risks that are part of the program

NOTE: All University departments are responsible for developing departmental operational procedures in support of this policy.

See the following pages for the full text of the policy.

Section 1 — Definitions

1. For purposes of this policy, the following definitions are applicable:
    A. Creditor: A person or entity that arranges for the extension, renewal, or continuation of credit, which in some cases could include third-party debt collectors.
    B. Consumer: An individual.
    C. Covered Account: An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions. Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to Customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks. Covered Account includes general activity relating to the tuition/fee or receivable billing, student loan origination and servicing, and ID card account maintenance.
    D. Customer: A person that has a "covered account" with a financial institution or creditor.
    E. Identity Theft: Fraud committed or attempted using the identifying information of another person without authority.
    F. Notice of Address Discrepancy: A notice sent to a user of a consumer report by a Consumer Reporting Agency pursuant to 15 U.S.C. 1681c(h)(1), that informs the user of a substantial difference between the address for the Consumer provided by the user in requesting the consumer report and the address or addresses the Consumer Reporting Agency has in the Consumer's file.
    G. Personally Identifiable Information: An individual's first name and last name and at least one of the following data elements: Social Security Number, driver's license number or identification card number, and account number, credit card number, debit card number, security code, access code, or password of an individual's Covered Account.
    H. Program: The Identity Theft Prevention Program.
    I. Red Flag: A pattern, practice, or specific activity that indicates the possible existence of identity theft.

Section 2 — Identity Theft Prevention Program

1. Covered accounts
    A. A covered account includes any consumer account that involves or is designed to permit multiple payments or transactions, such as a loan that is billed or payable monthly. Covered accounts include certain types of arrangements in which an individual establishes a "continuing relationship" with the University. Certain payment arrangements, such as payment of tuition in full at the beginning of the semester likely do not meet the "continuing relationship" standard.

B. Every new and existing account that meets the following criteria is covered by this program:
    i. Accounts for which there is a reasonably foreseeable risk of identity theft; or
    ii. Accounts for which there is a reasonably foreseeable risk to the safety or soundness of the University from identity theft, including financial, operational, compliance, reputation, or litigation risks.

2. Red flags
    A. The following red flags are potential indicators of fraud. Any time a red flag, or a situation closely resembling a red flag, is apparent, it should be investigated for verification.
        i. Alerts, notifications or warnings from a consumer reporting agency;
        ii. A fraud or active duty alert included with a consumer report;
        iii. A notice of credit freeze from a consumer reporting agency in response to a request for a consumer report; or
        iv. A notice of address discrepancy from a consumer reporting agency as defined in § 334.82(b) of the Fairness and Accuracy in Credit Transactions Act.
    B. Red flags also include consumer reports that indicate a pattern of activity inconsistent with the history and usual pattern of activity of an applicant or consumer, such as:
        i. A recent and significant increase in the volume of inquiries;
        ii. An unusual number of recently established credit relationships;
        iii. A material change in the use of credit, especially with respect to recently established credit relationships; or
        iv. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

3. Suspicious documents
    A. Documents provided for identification that appear to have been altered or forged.
    B. The photograph or physical description on the identification is not consistent with the appearance of the applicant or consumer presenting the identification.
    C. Other information on the identification is not consistent with information provided by the person opening a new covered account or consumer presenting the identification.
    D. Other information on the identification is not consistent with readily accessible information that is on file with the University, such as a signature card or a recent check.
    E. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

4. Suspicious personal identifying information
    A. Personal identifying information provided is inconsistent when compared against external information sources used by the University. For example:
        i. The address does not match any address in the consumer report;
        ii. The Social Security number (SSN) has not been issued or is listed on the Social Security Administration's Death Master File; or
        iii. Personal identifying information provided by the consumer is not consistent with other personal identifying information provided by the consumer. For example, there is a lack of correlation between the SSN range and date of birth.
    B. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the University. For example, the address on an application is the same as the address provided on a fraudulent application.
    C. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the University. For example:
        i. The address on an application is fictitious, a mail drop, or a prison; or
        ii. The phone number is invalid or is associated with a pager or answering service.
    D. The SSN provided is the same as that submitted by other persons opening an account or other consumers.
    E. The address or telephone number provided is the same as or similar to the address or telephone number submitted by an unusually large number of other consumers or other persons opening accounts.
    F. The consumer or the person opening the covered account fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.
    G. Personal identifying information provided is not consistent with personal identifying information that is on file with the University.
    H. When using security questions (mother's maiden name, pet's name, etc.), the person opening the covered account or the consumer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

5. Unusual use of, or suspicious activity related to, the covered account:
    A. Shortly following the notice of a change of address for a covered account, the University receives a request for new, additional, or replacement goods or services, or for the addition of authorized users on the account.
    B. A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example, the consumer fails to make the first payment or makes an initial payment but no subsequent payments.
    C. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:

i. Non-payment when there is no history of late or missed payments;
ii. A material change in purchasing or usage patterns

D. A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).
E. Mail sent to the consumer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the consumer's covered account.
F. The University is notified that the consumer is not receiving paper account statements.
G. The University is notified of unauthorized charges or transactions in connection with a consumer's covered account.
H. The University receives notice from consumers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the University.
I. The University is notified by a consumer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

Section 3 — Responding to Red Flags

1. Once potentially fraudulent activity is detected, the University must act quickly, as a rapid appropriate response can protect consumers and the University from damages and loss.
    A. Once potentially fraudulent activity is detected, gather all related documentation and write a description of the situation. Present this information to the designated authority for determination.
    B. The Information Security Officer, 773.508.7373, datasecurity@luc.edu is the designated authority.
    C. The designated authority will complete additional authentication to determine whether the attempted transaction was fraudulent or authentic.

2. If a transaction is determined to be fraudulent, appropriate actions must be taken immediately. Actions may include:
    A. Canceling the transaction;
    B. Notifying and cooperating with appropriate law enforcement;
    C. Determining the extent of liability of the University; and
    D. Notifying the actual consumer that fraud has been attempted.

Section 4 — Periodic Updates to Plan

1. The program will be re-evaluated periodically to determine whether all aspects of the program are up to date and applicable in the current business environment.

2. The periodic review will include an assessment of which accounts are covered by the program.

3. As part of the review, red flags may be revised, replaced or eliminated. Defining new red flags may also be appropriate.

Section 5 — Program Administration

1. Involvement of management
    A. The Identity Theft Prevention Program shall not be operated as an extension to existing fraud prevention programs, and its importance warrants the highest level of attention.
    B. Approval of the initial plan must be appropriately documented and maintained.
    C. Operational responsibility of the program is shared by Finance's Treasurer's Office and Information Technology Services.

2. Staff training
    A. Staff training shall be conducted by the Treasurer's Office and Information Technology Services for all employees and contractors for whom it is reasonably foreseeable that they may come into contact with accounts or personally identifiable information that may constitute a risk to the University or its consumers.
    B. Finance's Treasurer's Office and Information Technology Services share responsibility for ensuring identity theft training for all requisite employees and contractors.
    C. Employees and contractors who handle accounts covered by this policy must receive annual training in all elements of this policy.
    D. To ensure maximum effectiveness, employees and contractors may continue to receive additional training as changes to the program are made.

3. Oversight of service provider arrangements
    A. It is the responsibility of the University to ensure that the activities of all service providers are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.
    B. A service provider that maintains its own identity theft prevention program, consistent with the guidance of the red flag rules and validated by appropriate due diligence, may be considered to be meeting these requirements.
    C. Any specific requirements should be addressed in the appropriate contract arrangements.

Section 6 — Related Documents

1. Federal Register Final Rules:
    A. http://www.ftc.gov/os/fedreg/2007/november/071109redflags.pdf (contains definitions and final rules for 16 CFR 681.1, 681.2, and 681.3.)