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

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 Prv

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

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 a

2.

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.)