Loyola University Maryland
"Red Flag" Identity Theft Policy

PREAMBLE

Identity Theft

An identity can be stolen with nothing more than a stolen string of numbers and malicious intent. With a few pieces of personal identifying information, an identity thief can easily secure an account in someone

IDENTITY THEFT POLICY

SECTION 1: BACKGROUND

4. Cardholder address

4.A.1.b: Tax identification numbers, including:

1. Social Security number
2. Business identification number
3. Employer identification numbers

4.A.1.c: Payroll information, including, among other information:

3. Desks, workstations, work areas, printers and fax machines, and common shared work areas will be

3. A notice of credit freeze from a consumer reporting agency in response to a request for a consumer report; or

4. 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.

5.B.2: 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 customer, such as:

1. A recent and significant increase in the volume of inquiries;

2. An unusual number of recently established credit relationships;

3. A material change in the use of credit, especially with respect to recently established credit relationships; or

4. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

5.C: Suspicious documents

1. Documents provided for identification that appear to have been altered or forged.

2. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.

3. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.

4. Other information on the identification is not consistent with readily accessible information that is on file with the University.

5. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

5.D: Suspicious personal identifying information

1. Personal identifying information provided is inconsistent when compared against external information sources used by the University. For example:
   The address does not match any address in the consumer report;

   The Social Security number (SSN) has not been issued or is listed on the Social Security

   Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.

2. 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.

3. 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:

   The address on an application is fictitious, a mail drop, or a prison; or

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

4. The SSN provided is the same as that submitted by other persons opening an account or other customers.

5. 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 customers or other persons opening accounts.

6. The customer 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.

7. Personal identifying information provided is not consistent with personal identifying information that is on file with the University.

8. account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

5.E: Unusual use of, or suspicious activity related to, the covered account

1. 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.

2. A new student account is used in a manner commonly associated with known patterns of fraud patterns. For example, the student fails to make the first payment on their payment plan or makes an initial payment but no subsequent payments.

3. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:

   Nonpayment when there is no history of late or missed payments;

   A material change in registration/tuition charges or usage patterns.

4. 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).

5. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be

6. The University is notified that the customer is not receiving paper account statements.

7. covered account.

8. The University receives notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the University.

9. The University is notified by a customer, 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 6: RESPONDING TO RED FLAGS

6.A: Once potentially fraudulent activity is detected, an employee must act quickly as a rapid appropriate response can protect customers and the University from damages and loss.

1. 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.

2.

3. Operational responsibility of the program is delegated to the Director of Student Administrative Services (SAS).

8.B: Staff Training

1. Staff training shall be conducted for all employees, officials 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 customers.

2. The Director of SAS, is responsible for ensuring identity theft training for all requisite employees and contractors.

3. Employees must receive annual training in all elements of this policy.

4. To ensure maximum effectiveness, employees may continue to receive additional training as changes to the program are made.

8.C: Oversight of Service Provider Arrangements

1. 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.

2. 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.

3. Any specific requirements should be specifically addressed in the appropriate contract arrangements.

8.D: History/Revision Dates

Adopted by the Board of Trustees on April 11, 2012