University of La Verne

Purchasing and Procurement

UNIVERSITY POLICY FOR THE IDENTITY THEFT RED FLAGS RULE (May 2009)

Policy Statement
The University of La Verne endeavors to safeguard personal and private information of all of its constituents, including faculty, staff, students, vendors, and donors. Additionally, the University understands the importance of complying with applicable state and federal regulations enacted to prevent identity theft.

Purpose
The purpose of the University of La Verne's Identity Theft Program is to establish policies and procedures designed to detect, prevent and mitigate identify theft in those situations where the University or its suppliers and vendors have access to personal and private information that faculty, staff, students and donors or other third party customers or vendors wish to maintain confidential and not be disclosed to unauthorized persons. Such a program shall be considered in compliance with federal and state law so long as the policies and procedures are enacted properly and the persons responsible for implementing these policies and procedures regularly monitor any University transaction where confidential information is exchanged.

Definitions

Identity theft: means either fraudulently using or attempting to use the identifying information of another person without authority.

Covered Account: means any University sponsored or controlled account that involves having faculty, staff, students or donors undertake multiple payments or transactions, such as a loan or account that is billed or payable monthly, or an account or record that the University maintains for faculty, staff, students, or donors and where confidential and private or identifying information is collected and stored.

Red Flag: this means a pattern, practice, or specific activity that suggests or indicates the possible existence of identity theft.

Identifying Information: means any name or number that may be used, alone or in conjunction with any other information, that could be used to identify a specific person, including: name, address, telephone number, Social Security number, date of birth, government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, unique electronic identification number, computer's Internet Protocol (IP) address, or routing code.

The Program

The Program shall include reasonable policies and procedures to:

1. Identify relevant "Red Flags" for covered accounts the University offers or maintains; upon identifying these "Red Flags" the University shall then incorporate those "Red Flags" into the Program, as appropriate and reasonable.
2. Detect and record Red Flags that have been incorporated into the Program.
3. Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft.
4. Ensure the Program is updated periodically to reflect changes in identity theft risks to "customers" and to the safety and soundness of La Verne in its role as creditor.
5. Provide proper training to University staff to ensure that the foregoing policies and procedures are undertaken appropriately and that covered accounts are monitored properly to ensure compliance with University polices.

The Program shall, as appropriate, incorporate existing University policies and procedures that control reasonably foreseeable risks.

Administration of the Program

1. The Finance Office shall be responsible for developing and implementing the Program. Other administrative departments may be utilized, as needed, to ensure the Program is effectively and properly carried out.
2. University staff shall be trained, as necessary, to implement the Program effectively.
3. Notwithstanding the overall responsibility of the Finance Department to implement the Program, each University Department manager shall exercise appropriate and effective oversight of their service provider arrangements and ensure that staff and faculty adhere to the Program's requirements.
4. Knowledge about specific Red Flag identification markers, and certain detection, mitigation and prevention practices will be limited to those University staff that are responsible for administering this Program and to those University officials with a need to know them, including but not limited to the President of the University, and his or designees.

Identification of Relevant Red Flags

1. The Program shall include relevant "Red Flags" from the following categories as appropriate:
    a. Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services.
    b. The presentation of suspicious documents. (see Appendix A)
    c. The presentation of suspicious personal identifying information. (See Appendix B)
    d. The unusual use of, or other suspicious activity related to, a covered account. (See Appendix C)
    e. Notice received from staff, faculty, students, donors or "customers", or notices from victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts.
2. The Program shall consider the following risk factors in identifying relevant Red Flags for covered accounts as appropriate:
    a. The types of covered accounts offered or maintained by the University.
    b. The methods provided to open covered accounts by the University.

c. The methods provided to access covered accounts by the University.
d. The University's previous experience with identity theft.
e. The Program shall incorporate relevant Red Flags from sources such as:
f. Incidents of identity theft previously experienced.
g. Methods of identity theft that reflect changes in risk.
h. Applicable regulatory or professional guidance.

Detection of Red Flags

The Program shall address the detection of Red Flags in connection with the opening of covered accounts and existing covered accounts, such as by:

1. Obtaining identifying information about, and verifying the identity of, a person opening a covered account.

2. Authenticating the identity of a "customer", monitoring suspicious or unusual transactions, and verifying the validity of change of address requests in the case of existing covered accounts.

Response

The Program shall provide for timely and appropriate responses to detected Red Flags to prevent and mitigate identity theft. The response shall be commensurate with the degree of risk posed. Appropriate responses may include:

1. Monitor a covered account for evidence of identity theft.
2. Contact the person whose personal information may have been used by an unauthorized person
3. Change any passwords, security codes or other security devices that permit access to a covered account.
4. Reopen a covered account with a new account number.
5. Not open a new covered account.
6. Close an existing covered account.
7. Notify law enforcement.

8. Determine no response is warranted under the particular circumstances.

Updating the Program

The Program shall be updated periodically to reflect changes in risks to faculty, staff, students, donors or other persons who provide identifying information to the University, or to the safety and soundness of the organization from identity theft based on factors such as:

1. The experiences of the organization with identity theft.
2. Changes in methods of identity theft.
3. Changes in methods to detect, prevent and mitigate identity theft.
4. Changes in the types of accounts that the organization offers or maintains.
5. Changes in the business arrangements of the organization, including mergers, acquisitions, alliances, joint ventures and service provider arrangements.

Oversight of the Program

1. Oversight of the Program shall include:
    a. Assignment of specific responsibility for implementation of the Program.
    b. Review of reports prepared by staff regarding compliance.
    c. Approval of material changes to the Program as necessary to address changing risks of identity theft.

2. Reports shall be prepared as follows:
    a. Staff responsible for development, implementation and administration of the Program shall report to the Audit Committee at least annually on compliance by the organization with the Program.
    b. The report shall address material matters related to the Program and evaluate issues that include, but are not limited to the following: (i) effectiveness of the policies and procedures in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to

existing covered accounts; (ii) service provider agreements; (iii) significant incidents involving identity theft and the University's response to the incident(s) and (iv) recommendations for any material changes to the Program.

Oversight of Service Provider Arrangements

In any situation where the University engages a service provider to perform an activity in connection with one or more covered accounts, it will take the following steps to ensure the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of Identity Theft:

- Require, by contract, that service providers have identity theft policies and procedures in place; and
- Require, by contract, that service providers review the University's policies on maintaining the confidentiality of information and report any incidents that may be considered "Red Flags" to the appropriate University official.

APPENDIX A - Suspicious Documents

- Identification document or card that appears to be forged, altered or inauthentic;
- Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;
- Other document with information that is not consistent with existing customer information (such as if a person's signature on a check appears forged); and
- Application for service that appears to have been altered or forged.

APPENDIX B - Suspicious Personal Identifying Information

- Identifying information presented that is inconsistent with other information the customer provides (example: inconsistent birth dates);

• Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on the credit report);
• Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;
• Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);
• Social Security number presented that is the same as one given by another customer;
• An address or phone number presented that is the same as that of another person;
• A person fails to provide complete personal identifying information on an application when reminded to do so (however, by law social security numbers must not be required); and
• A person's identifying information is not consistent with the information that is on file for the customer.

APPENDIX C - Suspicious Account Activity or Unusual Use of Account

• Change of address for an account followed by a request to change the account holder's name;
• Payments stop on an otherwise consistently up-to-date account;
• Account used in a way that is not consistent with prior use (example: very high activity);
• Mail sent to the account holder is repeatedly returned as undeliverable;
• Notice to University that a customer is not receiving mail sent by the University;
• Notice to University that an account has unauthorized activity:
• Breach in University's computer system security; or
• Unauthorized access to or use of customer account information.