George Mason University
Identity Theft Prevention Program - Procedures
Revised September 30, 2012

Identification of Red Flags, Detecting Red Flags, and Preventing and Mitigating Identity Theft

IDENTIFICATION OF COVERED ACCOUNT RED FLAGS

In order to identify relevant Red Flags, the university considers the types of accounts that it offers and maintains, methods it provides to open its accounts, methods it provides to access its accounts, and its previous experiences with identity theft. The university identifies the following Red Flags in each of the listed categories:

A. Notifications and Warnings from Credit Reporting Agencies

Red Flags

1. Report of fraud accompanying a credit report;
2. Notice or report from a credit agency of a credit freeze on an applicant;
3. Notice or report from a credit agency of an active duty alert for an applicant; and
4. Indication from a credit report of activity that is inconsistent with an applicant's usual pattern or activity.

B. Suspicious Documents

Red Flags

1. Identification document or card that appears to be forged, altered or inauthentic;
2. Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;
3. Other document with information that is not consistent with existing student or employee information; and
4. Application that appears to have been altered or forged.

C. Suspicious Personal Identifying Information

Red Flags

1. Identifying information presented that is inconsistent with other information the student or employee provides (example: inconsistent birth dates);
2. Identifying information presented that is inconsistent with other sources of information (for instance, a name on a background check not matching a name on an employment application);
3. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent; and

4. Social security number presented that is the same as one given by another student or employee.

D. Suspicious Covered Account Activity or Unusual Use of Account

Red Flags

1. Notice to the university that a student or employee is not receiving email or mail sent by the university;
2. Notice to the university that an account has unauthorized activity;
3. Breach of a university's computer system security that provides access to covered accounts; and
4. Unauthorized access to or use of student or employee account information.

E. Alerts from Others

Red Flag

1. Notice to the university from a student, employee, identity theft victim, law enforcement or other person that the university has opened or is maintaining a fraudulent account for a person engaged in identity theft.

DETECTING RED FLAGS

A. Student Identification Cards

In order to detect any of the Red Flags identified above associated with issuing a photo ID for a student, university personnel will take the following step to obtain and verify the identity of the person opening the account:

Detect

1. Verify the student's identity at time of issuance of student identification card (review of driver's license or other government-issued photo identification).

B. Employment Eligibility Verification (Including Criminal and/or Financial Background Report Requests)

In order to detect any of the Red Flags identified above for an employment position whether or not a background report is sought, university personnel will take the following steps to obtain and verify the identity of the applicant:

Detect

1. Require certain identifying information such as name, date of birth, home address, SSN or other identification.
2. Verify the employee's identity at time of issuance of employee identification card (review of driver's license or other government-issued photo identification).
3. Process employment verifications for all new hires and rehires having a break in service greater than one year as defined by the Commonwealth of Virginia Department of Human Resource Management (DHRM) . This process for employment verifications (E-Verify) validates the information and supporting documents with Social Security Administration and Department of Home Land Security.

For an employment position for which a background report is sought, university personnel will take the following additional steps:

4. Compare the SSN provided by the applicant on the background check to the SSN reported on the Form I-9 which is input into Banner.
5. In the event of a SSN discrepancy, Employee Relations will discuss the discrepancy with the applicant.

C. Existing Accounts

In order to detect any of the Red Flags identified above for an existing Covered Account, university personnel will take the following steps to monitor transactions on an account:

Detect

1. Verify the identification of students or employees if they request information. If in person, require a photo ID; if via telephone, require the student ID number; via email, only respond to approved university email addresses;
2. Verify changes in banking information given for employee or student direct deposit purposes.

PREVENTING AND MITIGATING IDENTITY THEFT

In the event university personnel detect any identified Red Flags, such personnel shall take one or more of the following steps, depending on the degree of risk posed by the Red Flag:

Prevent and Mitigate

1. Continue to monitor a covered account for evidence of identity theft;
2. Contact the student or employee (by telephone if an email account is involved; by email otherwise) or applicant (for which a background check was run);
3. Deny access to (lock) covered accounts (LDAP, Patriot Web);
4. Not reopen a covered account until the event is investigated and risk mitigated;
5. Require the student or employee to reset their password;
6. Notify the appropriate Identity Theft Prevention Program committee member for determination of the appropriate step(s) to take;
7. Notify Campus Police or Internal Audit;

8. Assist in filing a Suspicious Activities Report ("SAR"), if requested by a financial institution required to file a SAR pursuant to the regulations of the Bank Secrecy Act;
9. Notify Department of Education Inspector General if financial aid is involved; or
10. Determine that no response is warranted under the particular circumstances.

Protect Student or Employee Identifying Information

In order to further prevent the likelihood of identity theft occurring with respect to covered accounts, the university will take the following steps with respect to its internal operating procedures to protect student or employee identifying information:
1. Ensure that Patriot Web is secure;
2. Ensure other university policies are in place to address secure destruction of paper documents and computer files containing student or employee account information when a decision has been made to no longer maintain such information;
3. Ensure that office computers with access to covered account information are password protected;
4. Avoid use of social security numbers;
5. Ensure computer virus protection is up to date;
6. Require and keep only the kinds of student or employee information that are necessary for university purposes.
7. Require that the first six digits and year of birth are masked in Banner and limit access to SSN and DOB to appropriate employees in the organization (i.e. Financial Aid, Human Resources, Payroll)
8. Ensure employees receive a confirmation email for changes in banking information for direct deposits.

ADMINISTERING THE PROGRAM

The initial program was approved by the Board of Visitors and is effective May 1, 2009. The Board of Visitors has designated the University Controller as the Program Administrator. The University Controller is designated with primary responsibility for oversight of the development, implementation, and administration of the Program and chairs the Identify Theft Committee.

The Committee is responsible for ensuring appropriate training of university staff on the Program, reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating identity theft, determining which steps of prevention and mitigation should be taken in particular circumstances, and considering periodic changes to the Program. The Committee also is responsible for providing an annual report of Program activity to the President, Senior Vice President and Provost.

An annual training program will be provided to all employees who process personal identifying information associated with covered accounts. The training program will be developed and administered at the department level.

Service providers used in connection with covered accounts, to include payment plan administrators and collection agencies, will be contacted annually to verify compliance with the Red Flags Rule.

This policy shall be reviewed and revised, if necessary, annually by the Committee to become effective at the beginning of the university's fiscal year, unless otherwise noted.