



Longwood University
President's Office
Chief Administration and Finance Officer
201 High Street, Lancaster 207, Farmville, VA 23909
Phone: 434.395.2016 Fax: 434.395.2635

IDENTITY THEFT PREVENTION PROGRAM PROCEDURES
(Reference Administrative Policy #1013)
Effective December 31, 2010

Longwood University is committed to identifying red flags associated with identity theft and protecting its students, faculty, staff and others who entrust their personal information with the University. The University complies with the FTC Red Flag Rule by developing Identify Theft Prevention Program procedures designed to assist University personnel in identifying, detecting and responding to red flags in an effort to prevent and mitigate identity theft in connection with covered accounts and to provide for continued administration of the Programs.

Student enrollment:

Admittance to the University and enrollment in undergraduate and graduate programs requires the following information: application with personally identifying information; high school/college transcripts; official ACT, SAT, Praxis I, GRE or GMAT scores; copy of teaching license (if applicable); personal statements and letters of recommendation. Enrollment in courses as a non-admitted student requires the following information: registration form with personally identifying information and official transcripts from previously attended institutions. *(Responsible Offices – Undergraduate and Graduate Admissions and Registrar)*

Employee hiring:

The application process requires non-student applicants to provide personally identifying information including schools/colleges attended and work history. Criminal background checks and prior employment references are completed on all applicants to be hired. Once hired, the I-9 process requires two identification documents. Employees are also required to provide a copy of their social security card for payroll purposes. Upon hiring, student workers must provide a photo ID, copy of their social security card, an I-9 Employment Eligibility form, tax forms and direct deposit authorization. These documents are submitted, along with an Employment/Payroll Authorization form signed by the student and hiring department representative, to the Student Employment Manager for verification and approval. No employees are paid without proper authorization. *(Responsible Offices – Human Resources, Student Employment Office and Payroll)*

Identifying Covered Accounts: Longwood University has identified the following covered accounts which are either administered by the University or administered by a service provider.

University covered accounts:

Student accounts with refund transactions – Personal student account payments and financial aid funds are applied directly to the student account. Funds that create an overpayment on the student account are refunded in the student’s name via direct deposit or check (as instructed by the student) and mailed to the student’s local or permanent address in Banner. Balances resulting from PLUS loans are refunded via check in the parent’s name and mailed to the address indicated on the loan application. No refund request is required; refunds are initiated by the University when an overpayment occurs. Students/parents may not request a check be issued otherwise. Loan accounts are maintained by the respective lending agencies. (*Responsible Office – Student Accounts*)

Emergency/short-term loans – Requests must be made in person to the Office of Financial Aid. Students applying for short-term loans must complete an application. A photocopy of their picture ID is attached to the application form. Loans are issued via check from Accounts Payable and can only be picked up in person in the Office of Financial Aid by showing picture ID, which is compared to the photocopy attached to the application form. The student is required to sign a promissory note prior to check receipt. The promissory note is submitted to the Student Accounts Office, and a charge is placed on the student account. The loan is repaid by disbursement of financial aid to the student account or in accordance with terms of the promissory note. (*Responsible Offices – Financial Aid and Student Accounts*)

LancerCard – The LancerCard is the official identification card for Longwood University. All students, faculty and staff members are eligible to receive a LancerCard and are issued an identification number. On the LancerCard is printed the name, picture and status of the individual. Before issuance of a LancerCard, the individual is identified in Banner or by Human Resources as to their status. Their identity is verified by checking a valid form of identification such as a driver’s license, military ID or passport. All LancerCards are issued in person and cannot be mailed or given to anyone other than the individual who is receiving the card. The LancerCard can also be used for meal plans, door access and Lancer CASH. Lancer CASH is a declining stored-value account that is accessed with the identification card. These accounts can be used at approved on-campus and off-campus merchant locations. Deposits can be made online with a credit card, at CSVT terminals, or at the LancerCard Office. Since the identification card is the method used to access the funds, the patron’s name and picture can be verified before or after the purchase. At unattended locations, daily limits are set to reduce the risk of abuse. The account holder can only spend up to the balance on their account; negative balances are not permitted. (*Responsible Office – LancerCard Office*)

Service provider covered accounts:

Student account payment plans – The University operates an in-house payment plan using TouchNet Systems software that interfaces with Banner. The software is user ID and password protected. The payment plan contract is set up by the student or authorized user entering required information, and payments are received via ACH. Longwood staff does not have access to the banking information set up by the student/authorized user; data is housed on a secure server at TouchNet Systems. (*Responsible Office – Student Accounts*)

Perkins loans – Perkins loans may be offered as part of the student’s financial aid package. Students accept Perkins loans by signing a Master Promissory Note. Promissory Notes are maintained in a locked, fire-proof file cabinet. Once in repayment status, student accounts are managed by the Student Accounts Office and a service provider, Campus Partners. (*Responsible Offices – Financial Aid and Student Accounts*)

Student accounts with collection agencies – Delinquent accounts are placed with various collection agencies. The University ensures that these agencies either comply with our Identity Theft Prevention Program or have their own policies and procedures to detect and respond to red flags. (*Responsible Office – Student Accounts*)

The University shall take appropriate steps to ensure that the activity of a service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft whenever the organization engages a service provider to perform an activity in connection with one or more covered accounts. Each department shall exercise appropriate and effective oversight of their service provider arrangement(s).

Detecting Red Flags: In identifying and detecting relevant red flags for covered accounts, the Program considers the types of covered accounts it offers or maintains, the methods provided to open and access covered accounts, and the University’s previous experiences with identity theft. The Program identifies the following red flags:

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 student or employee information; and
- Application that appears to have been altered or forged.

Suspicious Personal Identifying Information

- Identifying information presented that is inconsistent with other information the student or employee provides (examples: inconsistent birth dates, SSN not listed on SS Administration’s Master File);
- Identifying information presented that is inconsistent with other sources of information (example: a name or address on a background check not matching a name or address on an employment application);

- Identifying information presented that is the same as information shown on other applications that we found to be fraudulent;
- Request is made to mail something to an address not listed on file;
- Failure to provide complete identifying information as requested; and
- Social security number presented that is the same as one given by another student or employee.

Suspicious Covered Account Activity or Unusual Use of Accounts

- Unusual use of, or suspicious activity related to, a University covered account;
- Unusual requests to make changes to account information;
- Request for new or replacement card, or addition of authorized account users shortly following change of address notice;
- Attempts to redirect refund monies from destination identified in the system of record;
- Notice to the University that a student or employee is not receiving mail sent by the University;
- Mail is returned repeatedly as undeliverable although transactions continue to be conducted;
- Notice to the University that an account has unauthorized activity;
- Breach in the University's computer system security; and
- Unauthorized access to or use of student or employee account information.

Alerts from Others

- Notice to the University from a student, employee, service provider, identity theft victim, law enforcement authority, or other person regarding an actual or probable identity theft in connection with University covered accounts.

Mitigating Identity Theft: The Program will implement the following procedures designed to assist University personnel in identifying and detecting red flags relevant to opening, accessing or maintaining a covered account in an effort to prevent and mitigate identity theft:

- Obtain and verify the identity of student/staff prior to opening a covered account – require certain identifying information (name, birth date, academic records, home address, etc.) and check for inconsistent or incomplete information;
- Verify the student/staff identity at the time and identification card is issued;
- Authenticate student/staff when making changes to an existing covered account;
- Verify the validity of a change of address – encourage students and staff to make changes of address through the appropriate methods – if requested in person, require picture identification;
- Monitor transactions for possible red flags;
- Ensure paper documents associated with or containing covered account information and personally identifiable information on students and staff are maintained in a secure environment and shredded when retention requirements or the business need expire;

- Ensure electronic files containing covered account information and personally identifiable information are secured in accordance with University information security requirements, that access to such files is limited to those who need access to perform their job duties, and that such files and records within them are securely destroyed when retention requirements or the business need expire;
- Ensure that University websites used to access covered accounts meet University information security requirements;
- Collect social security numbers only if required or authorized by federal or state law;
- Verify identification of student or staff requesting personal identifying information or account information; and
- Verify an Information Release Consent Form or and Authorized User is on file prior to releasing any account information to anyone other than the student.

Responding to Red Flags: Employees are to report any known or suspected fraudulent activity immediately to the Vice President for Administration and Finance. One or more of the following steps shall be taken, depending on the degree of risk posed by the red flag:

1. Continue to monitor a covered account for evidence of identity theft;
2. Deny access to the covered account until other information is available to eliminate the red flag;
3. Investigate transactions and contact the student or employee to verify if activity is fraudulent;
4. Close the covered account;
5. Not open a new covered account until the event is investigated and risk mitigated;
6. Reopen a covered account with a new account number;
7. Change any passwords, security codes of other security devices that permit access to a covered account;
8. Notify law enforcement and/or internal audit;
9. Notify Department of Education Inspector General if financial aid is involved; or
10. Determine no response is warranted under the particular circumstances.

Administering the Program: The Vice President for Administration and Finance (VPAF) is responsible for Program administration, service provider arrangements, ensuring appropriate training of University staff on the Program, reviewing and staff reports regarding the detection of red flags, determining which steps of prevention and mitigation should be taken in particular circumstances and considering periodic changes to the Program. At least annually, the VPAF will review and update the Program to reflect changes in risks, taking into consideration the University's experiences with identity theft, changes in identity theft methods, changes in identity theft detection and prevention methods, changes in types of accounts the University maintains and changes in the University's business arrangements with other entities. After consideration of these factors, the VPAF will determine whether changes to the Program, including the listing of red flags, are warranted. The VPAF will utilize an Identity Theft Committee to assist in administration of the Program. Members of the committee may include representatives from Admissions, Registration, Human Resources, Payroll, Financial Aid, Student Accounts, the LancerCard Office, Graduate Office, International Studies and Information Security.