

W&L'S IDENTITY THEFT PREVENTION PROGRAM FOR EMPLOYEE AND STUDENT COVERED FINANCIAL ACCOUNTS AND LOANS

Q: WHY DID W&L ADOPT AN IDENTITY THEFT PREVENTION PROGRAM?

A: The Federal Trade Commission mandated that creditors and lenders who have loans and accounts involving multiple payments adopt a written Identity Theft Prevention Program for those loans and accounts, so W&L adopted this program to comply with the federal mandate.

Q: WHAT ACCOUNTS AND LOANS ARE COVERED?

A: Employee home loans, student tuition loans, loan repayment assistance programs, tuition payment plans, payroll advances, and employee and student accounts billed monthly (for purchases on University cards and other charges).

Q: WHAT TYPES OF TRANSACTIONS ARE NOT COVERED?

A: Financial transactions where the university is not a creditor or lender (e.g., direct deposit arrangements for paychecks, acceptance of checks or credit cards for bookstore purchases, donor gifts to W&L by check or credit card). Neither does the program apply to any non-financial transaction (e.g., transcript requests, alumni requests for name or address changes, requests for issuance of keys to campus offices, requests to give an employee or student access to sensitive or confidential information). However, all members of the campus community should use common sense and appropriate diligence in any transaction that could have information security or identity theft implications.

Q: IS THIS PROGRAM REALLY NECESSARY - - DOESN'T THE UNIVERSITY ALREADY VERIFY IDENTITY?

A: Because W&L has an employer-employee and/or student-educational institution relationship with employees and students, the university already has in place various identity verification measures under existing laws or programs (such as the I-9 work eligibility verification, National Student Clearinghouse verification of student information, and FAFSA verification for students applying for financial aid). Also, given the relatively small size of our campus population, university staff may have personal knowledge of the identity of employees and students who have covered loans and accounts. The provisions of this new program are intended only to supplement existing measures as may be appropriate for covered accounts or loans.

Q: WHAT DOES THE PROGRAM REQUIRE UNIVERSITY STAFF TO DO IF THEY DEAL WITH COVERED ACCOUNTS OR LOANS?

A: First, to identify red flags that are relevant to the particular types of accounts or loans that they handle, taking into consideration how accounts are opened and used. These red flags may include:

- receiving suspicious identification documents
- receiving inaccurate or inconsistent identifying information
- not receiving personal identifying information when requested
- experiencing suspicious account/loan activity
- being alerted to fraud or identity theft on a particular account.

Staff should take reasonable steps to verify identity on a student or employee opening a covered account or loan where there aren't already such steps taken. For example, if a university employee does not personally know a student who is requesting to have a university card issued, the employee should ask for a photo-ID before issuing the university card, because it can be used to charge purchases to a covered account. As another example, if an employee comes to the Business Office to arrange a payroll advance and the staff member assisting the employee does not have personal knowledge of his/her identity, the staff member should take reasonable steps to verify the person's identity (verifying date of birth, home address, asking for photo-ID, etc.)

Q: WHAT SHOULD STAFF DO IF THEY BECOME AWARE OF INFORMATION OR ACTIVITY INDICATING A POSSIBLE IDENTITY THEFT RED FLAG?

A: Staff should take reasonable steps as warranted by the situation. This may mean monitoring a loan or account, getting more information from the employee or student, changing passwords or access codes, declining to approve an account or loan transaction, or contacting the Treasurer/Vice President for Finance and Administration, Steve McAllister, x8942, to determine the appropriate steps to take.

Q: WHAT IF WE OUTSOURCE OPERATIONS CONNECTED TO COVERED LOANS OR ACCOUNTS?

A: If the university contracts with a service provide to perform services connected with a covered account or loan, the contract should require that the service provider will implement reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft and will report any detected red flags to the university. Please send the contract to the Office of General Counsel so that these provisions can be included.