4/30/09

BRADLEY UNIVERSITY IDENTITY THEFT PREVENTION PROGRAM

Program Adoption

Bradley University ("University") developed this Identity Theft Prevention Program ("Program") pursuant to the Federal Trade commission's Red Flags Rule ("Rule"), which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. The Program was developed with oversight and approval of the Vice President Business Affairs. After consideration of the size of the University's operations and account systems, and the nature and scope of the University's activities, the Vice President Business Affairs determined that this Program was appropriate for Bradley University, and therefore was approved on April 30, 2009, subject to review by the Audit Committee of the Board of Trustees in its July 2009 Board meeting.

Purpose

This Program is designed to detect, prevent and mitigate identity theft in connection with the opening of a covered account or an existing covered account and to provide for continued administration of the Program in compliance with Part 681 of Title 16 of the Code of Federal Regulations. This Program is unique to covered accounts while being part of overall University policies and procedures ensuring the identity of constituents of the University. The Program shall include reasonable policies and procedures to:

1. Identify relevant red flags for covered accounts it offers or maintains and incorporate those red flags into the program;
2. Detect 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; and
4. Ensure the Program is updated periodically to reflect changes in risks to Students and to the safety and soundness of the creditor from identity theft.

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

Red Flags Rule Definitions used in this Program

The Rule defines "Identity Theft" as "fraud committed using the identifying information of another person" and a "Red Flag" as a pattern, practice, or specific activity that indicates the possible existence of Identity Theft.

"Identifying information" is defined under the Rule as "any name or number that may be used, along or in conjunction with any other information, 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 address, or routing code. This would include both a student's university ID number and network ID number.

According to the Rule, the University is a creditor subject to the Rule requirements. The Rule defines creditors "to include finance companies, automobile dealers, mortgage brokers, utility companies, and telecommunications companies. Where non-profit and government entities defer payment for goods or services, they, too are to be considered creditors."

Covered Accounts

A "covered account" means an account that the University offers or maintains for personal, family or household purposes that involves or is designed to permit multiple payments or transactions. The University has identified six types of accounts, five of which are administered by the University and one type of account that is administered by a service provider.

University covered accounts:

1. Deferred Payment Plan
2. Monthly Installment Payment Plan
3. Refund of credit balances
4. Emergency, Woody and USX loans
5. Other employee installment payments made through payroll deduction for items such as personal computers, fitness center membership, parking permits.
6. All other business activities that may arise that result in multiple payments.

Service provider-covered account:

1. Perkins and Nursing Loan Program administered by ACS.

Identification of Relevant Red Flags

The Program considers the following risk factors in identifying relevant red flags for covered accounts:

1. The types of covered accounts as noted above.
2. The methods provided to open covered accounts –acceptance to the University and enrollment in classes may require all of the following information:
    a. Application with personally identifying information
    b. Promissory notes and Entrance Counseling papers with personally identifying information
    c. High school and college transcripts
    d. Official ACT or SAT scores
    e. Letters of recommendation
    f. Entrance Medical Record
    g. Immunization history
    h. Insurance card (international)
3. The methods provided to access covered accounts:

a. Disbursement obtained in person requires university picture identification.
b. Disbursements obtained by mail can only be mailed to an address on file.
c. Disbursements governed by payroll deductions can only be initiated by written consent with identification present.

4. The University's previous history of identify theft.

The Program identifies the following red flags, in each of the listed categories:

Suspicious Documents

1. Documents provided for identification appear to have been altered or forged.
2. The photograph or physical description on the identification card is not consistent with the appearance of the student presenting the identification;
3. A request made from a non-University issued e-mail account;
4. A request to mail something to an address not listed on file;
5. Other document with information that is not consistent with existing student information;
6. An application that appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled; and
7. Notice from students/employees, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts.

Suspicious Personal Identifying Information

1. Identifying information presented that is inconsistent with other information the student provides (example: inconsistent birth dates);
2. Identifying information presented that is inconsistent with other sources of information;
3. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;
4. Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious address);
5. Social security number presented that is the same as one given by another student;
6. An address or phone number presented that is the same as that of another person;
7. A person fails to provide complete personal identifying information on an application when reminded to do so; and
8. A person's identifying information is not consistent with the information that is on file for the student.

Suspicious Account Activity or Unusual Use of Account

1. Change of address for an account followed by a request to change the student's name;
2. Payments stop on an otherwise consistently up-to-date account;

3. Account used in a way that is not consistent with prior use;
4. Mail sent to student is repeatedly returned as undeliverable;
5. Notice to the University that a student is not receiving mail sent by the University;
6. Notice to the University that an account has unauthorized activity;
7. Breach in the University's computer system security; and
8. Unauthorized access to or use of student account information.

Alerts from Others: The University receives notice from students, employees, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft with covered accounts held by the University or notice from such parties that a fraudulent account has been opened for a person engaged in identity theft.

Responsibility for the Detection of Red Flags

Because of the nature of the University business, the Program delegates red flag detection as discussed above for each type of covered account as follows:

The Deferred Payment Plan (DPP)-requires 25% of the net semester charges by the first enrollment drop date. Remaining amount is payable in three equal installments over the course of the semester. This is the payment plan by default if payment is not made in full or the student hasn't elected the monthly payment plan. Some interim terms require 50% down and are paid in two installments. Bills are mailed to the permanent address on record. Effective May 2009, no bills will be mailed and electronic bills can be accessed through the student's portal with the student's BU net ID, security of which is governed by policy and procedure under the Department of Information Resources and Technology ("IRT"). Third party access to bills is the responsibility of the student and can be done electronically. **Red Flag** – The Admissions Department is responsible for detecting suspicious documents upon application and enrollment prior to a bill being generated. The IRT Department is responsible for securing personal identification information for network access to bills. The Registrar is responsible for securing identification before name and address changes. Student Fees personnel in the Controller's Office are responsible for monitoring suspicious account activity or unusual use of account.

The Monthly Installment Payment Plan (MIPP)-allows students to make monthly payments towards their charges. Each payment will be one-twelfth of the amount placed on installment. Enrollment in this plan is secured by a nonrefundable deposit. The University sends monthly bills which will be accessed only electronically, effective May 2009. Bills are accessed as described in DPP above. **Red Flag** – Same as those described in DPP above. Student Fees personnel are responsible for suspicious documentation upon enrollment in the plan.

Refund Credit Balances- must be initiated by the student by signing and returning the bill to the Controller's Office or electronically through the student portal. Effective May 2009, most refunds will be initiated electronically. The refund check can only be mailed

to the permanent address on record or picked up in person by showing their University picture ID. **Red Flag** – IRT Department is responsible for securing personal identification for network access. Student Fees personnel are responsible for verifying account balances and checking University picture ID before distributing refund check.

Emergency, Wood and USX Loans –only granted upon application and committee approval. Picture ID as well as proof of citizenship or VISA status is required. Controller's Office monitors the account. For USX and Woody loans, payment is made in 5 year installments beginning 1 year after the student ceases enrollment. For Emergency loans, payment is made in 3 monthly installments commencing 3 months after the loan is issued. **Red Flag** – Controller's Office staff are responsible for ID verification and account activity.

Payroll Deduction Programs – The University currently takes payroll deduction payments for gift pledges, parking permits, the personal computer loan program, University fitness/wellness center memberships, and infrequent employee receivables. All payment deductions are initiated with written consent of the employee. All payroll deductions are listed on the employee's payroll stub. **Red Flag** – Payroll Department is responsible for verification of employee's identification. Employee monitors with review of paystub.

Perkins and Nursing Loan Program - This program is administered by a third-party provider, ACS. ACS has provided the University with its Red Flag Policy with respect to activities it provides for the University and its Perkin Loan debtors. The University is responsible for awarding the loan, obtaining signed promissory notes and entrance counseling information, applying the loan proceeds to the student's tuition account, and for submitting all account information to ACS each semester. **Red Flag** – The Financial Aid Office is responsible for awarding the loan. It relies upon the verification of personal identification done by the Admissions Office. The Controller's Office applies the loan proceeds to the student's account via database exchange from the Financial Aid software system to the billing system. The IRT office is responsible for the integrity of both computer systems. The Controller's Office also monitors the accounts as administered by ACS. See *Oversight of Service Provider Arrangements.*

Response to Red Flags

The Program shall provide for appropriate responses to detected red flags to prevent and mitigate identity theft. The appropriate responses to the relevant red flags are as follows:

1. Deny access to the covered account until other information is available to eliminate the red flag;
2. Contact the student;
3. Change any passwords, security codes or other security devices that permit access to a covered account;
4. Notify the Program Administrator for determination of the appropriate step(s) to take;
5. Notify law enforcement; or

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

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 identifying information:

1. Ensure that its website is secure or provide clear notice that the website is not secure;
2. Ensure complete and secure destruction of paper documents and computer files containing student information;
3. Ensure that office computers are password protected and that computer screens lock after a set period of time;
4. Keep offices clear of papers containing student information;
5. Ensure computer virus protection is up to date;
6. Require and keep only the kinds of student information that is necessary for business purposes; and
7. Comply with all other University policies and procedures relating to the protection of personal information and prevention of identity theft (i.e., credit card security, social security number protection, FERPA and HIPPA privacy rules, document retention policy, etc.).

Oversight of the Program

Responsibility for developing, implementing and updating this Program lies with an Identity Theft Committee for the University. This Committee is headed by a Program Administrator who may be the Controller or his or her appointee. An individual appointed by the head of Admissions, Registrar's, IRT, Financial Aid and Campus Police comprise the remainder of the committee membership as well as the Student Finance Manager. The Program Administrator will be responsible for the Program administration, for ensuring appropriate training of University staff on the Program, for 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.

Updating the Program

This Program will be periodically reviewed and updated to reflect changes in risks to students and employees and the soundness of the University from identify theft. At least once per year, the Program Administrator will consider 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 considering these factors, the Program Administrator will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Program Administrator will update the Program.

Staff Training

University staff responsible for implementing the Program shall be trained either by or under the direction of the Identity Theft Committee or the Program Administrator in the detection of Red Flags, and the responsive steps to be taken when a Red Flag is detected.

Oversight of Service Provider Arrangements

The University shall take 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.

Currently the University uses ACS to administer the Perkins and Nursing Loan Programs. Students contact ACS directly through its website or by telephone and provide personally identifying information to be matched to the records that the University has provided to ACS.