UNIVERSITY OF SOUTHERN INDIANA

Board of Trustees Finance/Audit Committee Meeting
University Center - Conference Center
Saturday, 5/9/2009
11:00 am to 12:00 pm CT

1. APPROVAL OF RED FLAG POLICY

Rozewski Approve

The Federal Trade Commission (FTC) issued a regulation known as the Red Flags Rule intended to reduce the risk of identity theft. The University is subject to this regulation because, in the course of its normal business operations, it obtains various personal identifiers such as social security numbers. The new regulation requires a program be developed to protect such identifiers. Attachment A is the University's proposed Identity Theft Prevention Program, developed to assure compliance with this regulation.

Approval of the proposed Identity Theft Prevention Program (Attachment A) is recommended.

0509 F-A Attachment A - Identity Theft Prevention Program - Page 3

2. RECOMMENDATION TO APPROVE PROPOSED MISCELLANEOUS FEES FOR 2009-2010

Rozewski Approve

Miscellaneous Fees are those fees (other than the Contingent, Academic Facilities, Student Services, and Technology Fees) that are charged to some, but not necessarily all, students in the course of their attendance. Examples include, but are not limited to, Laboratory Fees, Parking Fees, and Late Registration Fees. A schedule of proposed Miscellaneous Fees is in Attachment B. The proposed Miscellaneous Fees for 2009-2010 are the same rates approved for 2008-2009.

Approval of a recommendation to the Board of Trustees to approve the proposed Miscellaneous Fees for 2009-2010 (Attachment B) is recommended.

NOTE: IC 21-14-2-7 requires state universities in Indiana to approve Mandatory Fees ("Tuition"), such as the Contingent, Academic Facilities, Student Services, and Technology Fees, for a two year period. Institutions must set those rates on or before June 30 of any odd-numbered year or 60 days after the state budget bill is enacted into law, whichever is later.

0509 F-A Attachment B Miscellaneous Fees 2009-2010 - Page 8

3. RECOMMENDATION TO APPROVE REQUEST FOR GENERAL REPAIR AND REHABILITATION FUNDS

Rozewski Approve

Approval of a recommendation to the Board of Trustees to approve the following request regarding funds for Repair and Rehabilitation of campus facilities is recommended.

It is expected that the Indiana General Assembly will appropriate funds for Repair and Rehabilitation of campus facilities in the current appropriations cycle, although the exact amount of appropriation will not be known prior to the distribution of this agenda. Attachment C is a list of projects totaling $3,325,000, some or all of which may be funded by such an appropriation, if it is received. The Board's pre-approval of this list positions the University to quickly implement projects when an appropriation is received. Projects on the list not funded in the current appropriation cycle will be held over for inclusion on a future project list or completed using other University resources.

0509 F-A Attachment C - Repair and Rehabilitation and Infrastructure List - Page 9

4. REPORT OF CHANGE ORDERS ISSUED BY THE VICE PRESIDENT FOR BUSINESS AFFAIRS

Rozewski Present

Attached is a list (Attachment D) of construction change orders approved by the vice president for Business Affairs.

0509 F-A Attachment D - Summary of Construction Change Orders - Page 10

5. APPROVAL OF CHANGE ORDERS

Rozewski Approve

Approval of the construction change orders in Attachment E (which require the approval of the committee) is recommended.

0509 F-A Attachment E Summary of Construction Change Orders over $25k - Page 12

Attachment A
UNIVERSITY OF SOUTHERN INDIANA
Identity Theft Prevention Program

Approval of the following proposed Identity Theft Prevention Program is recommended.

I. PROGRAM ADOPTION
The University of Southern Indiana developed this Identity Theft Prevention Program ("Program") pursuant to the Federal Trade Commission's ("FTC") Red Flags Rule, which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. After consideration of the size and complexity of the University operations and account systems, and the nature and scope of its activities, the University determined that this Program is appropriate.

II. PURPOSE
The purpose of this policy is to establish an Identity Theft Prevention Program 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. 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.

III. DEFINITIONS AND PROGRAM

A. Red Flags Rule Definitions Used in this Program

"Identity Theft" is a "fraud committed or attempted using the identifying information of another person without authority."

A "Red Flag" is a "pattern, practice, or specific activity that indicates the possible existence of Identity Theft."

A "Covered Account" is an account the University maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions.

The "Program Administrator" is the individual designated with primary responsibility for oversight of the program. See Section VI below.

"Identifying information" is "any name or number that may be used, alone 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, student identification number, computer's Internet Protocol address, or routing code.

B. Fulfilling Requirements of the Red Flags Rule

Under the Red Flags Rule, the University is required to establish an "Identity Theft Prevention Program" tailored to its size and complexity and the nature of its operation. The program must contain reasonable policies and procedures to:

1. Identify relevant Red Flags for new and existing covered accounts 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 or to the safety and soundness of the student from Identity Theft.

IV. COVERED ACCOUNTS

The University has identified types of accounts, of which are covered accounts administered by the University and a number of accounts that are administered by a service provider.

Covered accounts:

1. EXAMPLE - Refund of credit balances involving PLUS loans
2. EXAMPLE - Refund of credit balances without PLUS loans
3. EXAMPLE - Deferment of tuition payments
4. EXAMPLE - Emergency loans
5. EXAMPLE - Bookstore charges
6. EXAMPLE - Student Health Center charges
7. EXAMPLE - Student enrollment information
8. EXAMPLE - Student Financial Aid information
9. EXAMPLE - Student/Employee personnel data
10. EXAMPLE - Student placement data (can only be released with written permission of the student/client)

V. 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 campus and enrollment in classes requires all of the following information:
    a. Common application with personally identifying information
    b. High school transcript
    c. Official ACT or SAT scores
    d. Two letters of recommendation
    e. Entrance Medical Record
    f. Medical history
    g. Immunization history
    h. Insurance card
3. The methods provided to access Covered Accounts:
    a. Disbursement obtained in person require picture identification
    b. Disbursements obtained by mail can only be mailed to an address on file
4. The University's previous history of Identity Theft.

The University has identified 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;
4. Receipt of a notice of address discrepancy in response to a credit report request; and
5. 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 information; and
4. Application for service 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 provides (example: inconsistent birth dates);
2. Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a loan application);
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 billing 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.

D. Suspicious Covered Account Activity or Unusual Use of Account

Red Flags

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 the student is repeatedly returned as undeliverable;
5. Notice that a student is not receiving mail sent by the University;
6. Notice 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.

E. Alerts from Others

Red Flag

Notice to the University from a student or employee, Identity Theft victim, law enforcement, or other person that it has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.

VI. DETECTING RED FLAGS

A. Student Enrollment

In order to detect any of the Red Flags identified above associated with the enrollment of a student, personnel will take the following steps to obtain and verify the identity of the person opening the account:

Detect

1. Require certain identifying information such as name, date of birth, academic records, home address, or other identification; and
2. 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. 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 if they request information (in person, via telephone, via facsimile, via email);
2. Verify the validity of requests to change billing addresses by mail or email and provide the student a reasonable means of promptly reporting incorrect billing address changes; and
3. Verify changes in banking information given for billing and payment purposes.

C. Consumer ("Credit") Report Requests

In order to detect any of the Red Flags identified above for an employment or volunteer position for which a credit or background report is sought, personnel will take the following steps to assist in identifying address discrepancies:

1. Require written verification from any applicant that the address provided by the applicant is accurate at the time the request for the credit report is made to the consumer reporting agency; and
2. In the event that notice of an address discrepancy is received, verify that the credit report pertains to the applicant for whom the requested report was made and report to the consumer reporting agency an address for the applicant that the University has reasonably confirmed is accurate.

VII. PREVENTING AND MITIGATING IDENTITY THEFT

In the event 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 applicant (for whom a credit report was run);
3. Change any passwords or other security devices that permit access to Covered Accounts;
4. Not open a new Covered Account;
5. Provide the student with a new student identification number;
6. Notify the Program Administrator for determination of the appropriate step(s) to take;
7. Notify law enforcement;
8. File or assist in filing a Suspicious Activities Report ("SAR"); or
9. Determine that no response is warranted under the particular circumstances.

Protect Student 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 identifying information:

1. Ensure its website is secure or provide clear notice the website is not secure;
2. Ensure complete and secure destruction of paper documents and computer files containing student 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; and
6. Require and keep only the kinds of student information necessary for operational purposes.

VIII. PROGRAM ADMINISTRATION

A. Oversight

Responsibility for developing, implementing, and updating this Program lies with an Identity Theft Committee ("Committee") which will be a subcommittee of the Computer Advisory Committee. The Committee is headed by a Program Administrator who may be the Computer Center Director or his or her appointee. Two or more other individuals appointed by the President comprise the remainder of the committee. The Program Administrator will be responsible for ensuring appropriate training of staff on the Program, reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating Identity Theft, and determining which steps of prevention and mitigation should be taken in particular circumstances and considering periodic changes to the Program.

B. Staff Training and Reports

Staff responsible for implementing the Program shall be trained either by or under the direction of the Program Administrator in the detection of Red Flags and the responsive steps to be taken when a Red Flag is detected. Staff shall be trained, as necessary, to effectively implement the Program. University employees are expected to notify the Program Administrator once they become aware of an incident of Identity Theft or of the failure to comply with this Program. At least annually or as otherwise requested by the Program Administrator, staff responsible for development, implementation, and administration of the Program shall report to the Program Administrator on compliance with this Program. The report should address such issues as effectiveness of the policies and procedures in addressing the risk of Identity Theft in connection with the opening and maintenance of Covered Accounts, service provider arrangements, significant incidents involving Identity Theft and management's response, and recommendations for changes to the Program.

C. Service Provider Arrangements

In the event the University engages a service provider to perform an activity in connection with one or more Covered Accounts, the University 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:

1. Require, by contract, that service providers have such policies and procedures in place; and
2. Require, by contract, that service providers review the University's Program and report any Red Flags to the Program Administrator or the employee with primary oversight of the service provider relationship.

D. Non-disclosure of Specific Practices

For the effectiveness of this Identity Theft Prevention Program, knowledge about specific Red Flag identification, detection, mitigation, and prevention practices may need to be limited to the Committee which developed this Program and to those employees with a need to know. Any documents that may have been produced or are produced in order to develop or implement this program that list or describe such specific practices and the information those documents contain are considered confidential and should not be shared with other employees or the public. The Program Administrator shall inform the Committee and those employees with a need to know the information of those documents or specific practices which should be maintained in a confidential manner.

E. Program Updates

The Committee will periodically review and update this Program to reflect changes in risks to students and the soundness of the University from Identity Theft. In doing so, the Committee will consider the campus experiences with Identity Theft situations, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, and changes in the campus 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 Committee will update the Program.

Attachment B

Approval of the following miscellaneous fees is recommended.

MISCELLANEOUS FEES
2009-2010

1. LABORATORY AND MISCELLANEOUS FEES

	Current Fee	Proposed Fee	Effective Date
Application Fee	25.00	25.00	08/31/09
Audit Fee (plus applicable lab fee)	35.00	35.00	08/31/09
Computer Lab Fee	35.00	35.00	08/31/09
Departmental Exams Fee	15.00	15.00	08/31/09
Distance Education Fee (Learning Center Fee, per credit hour)	25.00	25.00	08/31/09
Distance Education Delivery Fee (per credit hour)	10.00	10.00	08/31/09
Distance Education Supply Fee	100.00	100.00	08/31/09
Health Professions Insurance	15.00	15.00	08/31/09
Health Services Fee	47.00	47.00	08/31/09
Laboratory Fee (College of Science and Engineering)	45.00	45.00	08/31/09
Laboratory Fee (all other colleges)	35.00	35.00	08/31/09
Late Registration Fee Week 1	30.00	30.00	08/31/09
Late Registration Fee Beginning Week 2	125.00	125.00	08/31/09
Matriculation Fee (all students)	65.00	65.00	08/31/09
Nursing Test Fee	30.00	30.00	08/31/09
Occupational Therapy Clinical Fee	50.00	50.00	08/31/09
Payment Plan Fee	30.00	30.00	08/31/09
Payment Plan Late Fee	25.00	25.00	08/31/09
Physical Education Fee	25.00	25.00	08/31/09
Respiratory Therapy Advanced Life Support Fee	100.00	100.00	08/31/09
Special Course Fee (varies by course; maximum amount)	200.00	200.00	08/31/09
Student Activity Fee (non-mandatory)	25.00	25.00	08/31/09
Studio Fee	35.00	35.00	08/31/09
Study Abroad Fee	100.00	100.00	08/31/09
Transportation and Parking Fee (8 or more credit hours per semester)	50.00	50.00	08/31/09
Transportation and Parking Fee (More than 3 and fewer than 8 credit hours per semester)	40.00	40.00	08/31/09
Transportation and Parking Fee (3 or fewer credit hours)	30.00	30.00	08/31/09

Attachment C

Approval of the following proposed Repair and Rehabilitation and Infrastructure Projects is recommended.

University of Southern Indiana
General Repair and Rehabilitation and Infrastructure Projects

1.	**Science Center Renovation – Phase 4** • Renovate the second floor of the 1968 Science Center. Phases 1, 2, and 3 renovated the third floor of the three-story building and are complete.	**$ 900,000**
2.	**Science Center Roof Replacement**	**$ 150,000**
3.	**Physical Activities Center Roof Replacement**	**$ 300,000**
4.	**Repair, Replacement, and Extension of Walkways and Bikeways** • Design is complete for Phase 1 of the proposed work, the replacement of walks in the core of campus between the Orr Center and University Center. Design is almost complete for Phase 2, the extension of a pedestrian/bike path from the academic core to the outdoor athletic complex.	**$ 700,000**
5.	**Upgrade Energy Management Systems** • Upgrade of the Energy Management Systems in the Health Professions Center, Technology Center, Liberal Arts Center, Physical Plant, Science Center, Orr Center, and Physical Activities Center.	**$ 365,000**
6.	**Repave University Boulevard** • Repave University Boulevard between Bent Twig Lane and Rice Library.	**$ 100,000**
7.	**Upgrade Fire Alarm System** • Upgrade the Fire Alarm System in the Technology Center.	**$ 35,000**
8.	**Replace the New Harmony Atheneum HVAC System** • Replace the New Harmony Atheneum HVAC System.	**$ 400,000**
9.	**Renovate Natatorium** • Repaint walls and ceilings and resurface pool deck.	**$ 300,000**
	TOTAL	**$3,325,000**

Attachment D

Summary of Construction Change Orders
Authorized by the Vice President for Business Affairs

1. RECREATION AND FITNESS CENTER EXPANSION PROJECT

Arc Construction Company – General Construction Contractor

CO G-4	Install glazed concrete block, ebony color, around stairway in Free Weight Room	$ 2,500
CO G-5	Paint front entrance bulkheads per PR G-13	
	Omit inlaid floor logos per PR G-20	
	Furnish and install butt glazing clips on glass at climbing wall	$ 2,700
CO G-6	Perform additional work in existing building including:	
	Remove block and install floor covering around columns at basketball court per PR G-10	
	Remove existing carpet in Storage 108	
	Additional painting of walls at Basketball Courts and Hall 101B per PR G-24	$15,025
CO G-7	Furnish and install steel structure from ceiling in climbing wall for belaying	
	Furnish and install storage cabinet at climbing wall	$18,090

Mel-Kay Electric Company – Electrical Contractor

CO E-4	Furnish and install camera above ITS Room	
	Install four light fixtures in Room 110 and Room 111	$ 5,996

2. BUSINESS AND ENGINEERING CENTER PROJECT

SUPPORT SERVICES BUILDING
Key Construction Company – Contractor

CO 11	Add two indoor and one outdoor camera(s) to security system	
	Add light switches in Rooms 105 and 109, including materials per PR 20 and PR30	$14,540

3. UNIVERSITY CENTER EXPANSION PROJECT

CO 003	Delete removal of air handling unit from demolition to allow asbestos removal	
	General Construction - Weddle Brothers Construction Co.	($6,131)
	Mechanical Construction - Deig Brothers Construction Co.	0
	Electrical Construction - Capital Electric Co.	0
CO 004	Change electrical systems to connect automatic flush valves in restrooms to emergency power system	
	General Construction - Weddle Brothers Construction Co.	$0
	Mechanical Construction - Deig Brothers Construction Co.	$0
	Electrical Construction - Capital Electric Co.	$0
CO 005	Delete sprinkler system from tower area, Room 2201	
	General Construction - Weddle Brothers Construction Co.	$0
	Mechanical Construction - Deig Brothers Construction Co.	($490)
	Electrical Construction - Capital Electric Co.	$0

Attachment E

Summary of Construction Change Orders for Approval of the Finance/Audit Committee

Approval of the following construction change orders is recommended.

1. UNIVERSITY CENTER EXPANSION PROJECT

CO 001 Add Bid Alternate 6, Supplemental Site Work and Landscaping, into the construction contracts

General Construction - Weddle Brothers Construction Co.	$170,000
Mechanical Construction - Deig Brothers Construction Co.	$430
Electrical Construction - Capital Electric Co.	$7,375

CO 002 Replace electrical and control service (to be demolished in project) for Parking Lot C lighting, exterior lighting at site, and Rice Plaza lighting

General Construction - Weddle Brothers Construction Co.	$0
Mechanical Construction - Deig Brothers Construction Co.	$1,540
Electrical Construction - Capital Electric Co.	$39,482