IDENTITY THEFT PREVENTION PROGRAM TRAINING MODULE

February 2009

Table of Contents

Introduction to the Training Module

This training module is a required component of the University of Missouri’s Identity Theft Prevention Program (ITPP).

These slides are intended to ensure that staff are knowledgeable and are able to take steps to detect, prevent and mitigate theft of personally identifiable financial information of the University’s customers to the extent reasonably possible.

University employees working for departments subject to the ITPP program, who are involved in the creation, modification or administration of covered accounts, are required to review this presentation and successfully complete the accompanying test.

Introduction to the Training Module

To complete this module:

1. Read and understand the information presented herein.
2. If necessary, refer to the Identity Theft Prevention Program, which is available at http://www.umsystem.edu/ums/departments/fa/itpp/.
3. This presentation is accompanied by a “mastery test” that must be completed by answering 80% or more of the questions correct.
4. Staff may repeat the mastery test until the 80%+ criterion has been accomplished. (Staff may review the training module as necessary to complete the mastery test.)
5. When item #3 is accomplished, a certificate will appear which staff must download and sign.
6. Staff will provide this certificate to their supervisor as a signed acknowledgement that they have completed the training.

I. INTRODUCTION

The Fair and Accurate Credit Transactions (FACT) Act of 2003 amended the Fair Credit Reporting Act, and required the Federal Trade Commission (FTC), together with other regulatory agencies, to issue and enact regulations requiring financial institutions and creditors to develop and implement written **identity theft prevention programs (ITPP).**

The regulations apply to the University of Missouri because it is a "**creditor**" - defined as any person who defers payment for services rendered.

I. INTRODUCTION

The University has developed and implemented a program for **the identification, detection, prevention and mitigation** of theft of personally identifiable financial information in covered accounts, defined as those accounts where multiple payments or transactions are permitted.

The University of Missouri's ITPP was approved by the Board of Curators on February 6, 2009.

II. DEFINITIONS

Account: A continuing relationship established by a person with the University to obtain a product or service for personal, family, household or business purposes. This includes an extension of credit, such as the purchase of services involving a deferred payment.

Covered Account: an account that the University offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, or any other account that the University offers or maintains for which there is a reasonably foreseeable risk to customers from identity theft. A covered account includes certain types of arrangements in which an individual establishes a "continuing relationship" with the University, including billing for previous services rendered.

II. DEFINITIONS

Customer: a person that has a covered account with the University of Missouri.

Identifying Information: information, such as a name or number, that may be used, alone or in conjunction with other information, to identify a specific person. Identifying information can include a person's name, address, telephone number, social security number, birth date, driver's license number, student identification number, or passport number.

Identity Theft: fraud or theft committed or attempted using the personal identifying information of another person without that person's authority.

II. DEFINITIONS

Red flag: a pattern, practice or specific activity that indicates the possible existence of identity theft.

Service Provider: any person or entity that provides a service to the University.

Workplace Information Security Manual (WISM): a checklist which department administrators must complete, designed to identify and correct weaknesses in the area of information security within a given department or workplace.

III. RECOGNIZING IDENTITY THEFT

The following should be considered in identifying relevant red flags:

1. The types of covered accounts offered or maintained;
2. The methods provided to open covered accounts;
3. The methods provided to access covered accounts; and
4. Previous experiences with identity theft

IV. IDENTIFYING IDENTITY THEFT

The following are five categories of Red Flags. Within each category are examples of Red flags that should be considered in identifying relevant Red Flags:

1. An alert, notification or warning from a consumer reporting agency*
2. Suspicious documents*
3. Suspicious personal identifying information*
4. Unusual use of, or suspicious activity related to, a covered account*
5. The University is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that the covered account is being used for identity theft.

- More detailed information is provided on the following pages and is available in the Identity Theft Prevention Program (ITPP) at http://www.umsystem.edu/ums/departments/fa/itpp/.

IV. IDENTIFYING IDENTITY THEFT

1. **An alert, notification or warning from a consumer reporting agency**

Examples:

a. a fraud or active duty alert
b. a credit freeze in response to a request for a consumer report

IV. IDENTIFYING IDENTITY THEFT

2. Suspicious documents

Examples:

a. Documents provided for identification that appear to have been altered or forged, or give the appearance of having been destroyed and reassembled;

b. A photograph or physical description on an identification that is not consistent with the appearance of the person presenting the identification;

c. Information on the identification that is not consistent with information provided by the person opening a new covered account or presenting the identification;

d. Information on the identification that is not consistent with readily accessible information that is on file with the University, such as a signature card or a recent check.

IV. IDENTIFYING IDENTITY THEFT

3. Suspicious personal identifying information

Examples:

a. Personal identifying information provided by the customer:
   i. is not consistent when compared against external information sources;
   ii. is not consistent with other personal identifying information provided by the customer;
   iii. is associated with known fraudulent activity;
   iv. is of a type commonly associated with fraudulent activity;
   v. is not consistent with personal identifying information that is on file with the University.

b. The social security number provided is the same as that submitted by other customers;

c. The address or telephone number provided is the same or similar to the address or phone number submitted by an unusually large number of other persons;

d. The person opening the covered account fails to provide all required personal identifying information on an application or upon request of the University.

IV. IDENTIFYING IDENTITY THEFT

4. Unusual use of, or suspicious activity related to, a covered account

Examples:

a. Shortly following the notice of a change of address of a covered account, the University receives a request for the addition of authorized users on the account;

b. The covered account is used in a manner that is not consistent with established patterns of activity;

c. Mail sent to the customer is returned repeatedly as undeliverable, although the customer continues to accrue charges on the covered account;

d. The University is notified of unauthorized changes or transactions in connection with a customer's covered account.

V. DETECTING IDENTITY THEFT

To Detect Red Flags Associated with the Opening of a New Covered Account:

Personnel will take the following steps to obtain and verify the identity of the person opening the account:

1. Require certain identifying information, such as name, date of birth, home address or other identification; and
2. Verify the individual’s identity by reviewing a driver’s license or other government issued photo identification.

V. DETECTING IDENTITY THEFT

To Detect Red Flags Associated with an Existing Covered Account:

Personnel will take the following steps to monitor transactions on the account:

1. Verify the identification of the individual if he/she requests information either in person, via telephone, facsimile or email;
2. Verify the validity of any requests to change billing addresses by mail or email and provide the individual with a means of promptly reporting incorrect billing address changes; and
3. Verify changes in banking information given for billing and payment purposes.

VI. MITIGATING IDENTITY THEFT

If University personnel detect possible identity theft, they should take one or more of the following steps:

1. Contact the person who "owns" the covered account;
2. Change any passwords or other security devices that permit access to Covered Accounts;
3. Continue to monitor activity on the Covered Account;
4. Notify their supervisor to determine additional steps needed;
5. Notify law enforcement after consultation with the business unit's Identity Theft Prevention Committee representative* and/or Office of the General Counsel.

*More detailed information on the Identity Theft Committee is available in the Identity Theft Prevention Program (ITPP) at http://www.umsystem.edu/ums/departments/fa/itpp/.

VII. PREVENTING IDENTITY THEFT

To protect Covered Accounts from identity theft, ensure that:

- Any University website that is used to access Covered Accounts is secure or provide clear notice to all users that the website is not secure.
- Paper documents which contain personal identifying information are maintained in a secure environment, and such documents are shredded when the University no longer needs to retain them.
- Computer files containing personal identifying information are secure and that the only individuals who have access to such files are those with a need to access the files in order to perform their job duties.
- All office computers which store or access Covered Account information must be password protected and must follow all other computer security best practices as established by the University's information security program*.

* BPM 1203

VII. PREVENTING IDENTITY THEFT

- **Ensure that any University website that is used to access Covered Accounts is secure or provide clear notice to all users that the website is not secure.**

Examples:

o Departmentally controlled IT resources (network, servers, applications, individual workstations, etc.) are maintained in strict compliance with the UM Information Security Program best practices (*see Note).

* BPM 1203

VII. PREVENTING IDENTITY THEFT

- **Ensure that paper documents which contain personal identifying information are maintained in a secure environment, and such documents are shredded when the University no longer needs to retain them.**

Examples:

- Employees keep sensitive documents and working materials out of the public view while working.
- Sensitive documents and working materials are secured during breaks and non-working hours.
- File cabinets that contain sensitive or confidential documents are located in a secure area.
- Employees are trained or otherwise required to use shredders for sensitive or confidential documents.

VII. PREVENTING IDENTITY THEFT

- **Ensure that computer files containing personal identifying information are secure and that the only individuals who have access to such files are those with a need to access the files in order to perform their job duties.**

Examples:

- Computer files containing sensitive or confidential information are stored in a secure manner.
- There are adequate procedures in place to ensure that only necessary access to information system resources are made available to employees to perform their job (principle of least privilege).

VII. PREVENTING IDENTITY THEFT

- **Ensure that all office computers which store or access Covered Account information must be password protected and must follow all other computer security best practices as established by the University's information security program*.**

Examples:

- Employees are required to use a strong password for access to their computer and other systems.
- Employees are required to lock their computers and/or use password protected screensavers when they leave their work area.
- If employees are allowed to work remotely (e.g., from home or while traveling), secure methods are used to access IT resources and transmit files (e.g., the use of VPN, security of laptops, encryption, etc.).

* BPM 1203

VII. PREVENTING IDENTITY THEFT

Audit Requirements:

1. Each department subject to this program:
   a. Should perform periodic audits to ensure that individuals who should not have access to such files are not accessing them.
   b. Must perform an annual risk assessment by completing the Workplace Information Security Manual (WISM).
2. The completed WISM must be returned to the appropriate business unit's Identity Theft committee member, who will review the WISM and will forward it to the UM System Coordinator.
3. The UM System Coordinator and the UM Chief Information Security Officer (CISO) will be responsible for reviewing each completed WISM and will identify unresolved security risks that departments must address.

Incidents of Identity theft:

Incidents of identity theft must be reported to the UM System Coordinator.

VIII. PROGRAM ADMINISTRATION

Oversight:

- Responsibility for developing, implementing and updating this Program lies with the Program Administrator, who is appointed by The Curators of the University of Missouri. The Program Administrator is the Vice President for Finance and Administration.

- The Program Administrator has designated an Identity Theft Prevention Program Committee for the University and has appointed members to this committee. Members include a UM System Coordinator, a representative from the Office of the Vice President for Information Technology, and representatives from each campus and UMHC. A representative from the Office of the General Counsel serves as an ex officio member of the Identity Theft Prevention Program (ITPP) Committee. ITPP committee members are responsible for the implementation of the ITPP activities.

VIII. PROGRAM ADMINISTRATION

Training Requirements:

Each department subject to this program must complete training to effectively implement the ITPP. This includes:

- Successful completion of this training module by all staff who are involved in the creation, modification or administration of covered accounts to ensure that these staff are knowledgeable and are able to take steps to detect, prevent and mitigate theft of personally identifiable financial information of the University's customers to the extent reasonably possible.
- Departmental completion of the WISM and the successful resolution of any security risks identified.
- Information security awareness training, which is required for all staff working in offices affected by this program. Training can be obtained by contacting the Information Security Officer (ISO) at each business unit. A listing of the ISOs can be found at http://www.umsystem.edu/ums/departments/is/infosec/iso.shtml.