Tab 20

Missouri Student Loan Program Identity Theft Prevention Program

Coordinating Board for Higher Education
September 15, 2021

BACKGROUND

According to the Federal Trade Commission, an estimated nine million Americans have their identities stolen each year. The Red Flags Rule was first issued in 2007 under Section 114 of the Fair and Accurate Credit Transaction Act of 2003, and it was amended in 2010 by the Red Flags Program Clarification Act of 2010. The rule requires creditors to identify risks that may indicate potentially fraudulent activity, and to implement a written identity theft prevention program.

The Missouri Student Loan Program (MSLP) operated by the Department of Higher Education and Workforce Development is considered a creditor subject to the rule requirements, and as such, all of the MSLP's guaranteed student loan accounts are covered by the rule. The rule defines creditors "to include finance companies, automobile dealers, mortgage brokers, utility companies, and telecommunication companies. Where non-profit and government entities defer payment for goods or services, they, too, are to be considered creditors."

The MSLP first developed an Identity Theft Prevention Program in 2008. The loan program did not have a staff person specifically responsible for information security at that time, so it appears the original program was developed by the Director of the MSLP. The Coordinating Board approved the Identity Theft Prevention Program, and it became effective on November 1, 2008. The program has not been updated since that time.

CURRENT STATUS

The DHEWD Information Security Senior Associate and the Director of the MSLP worked with other loan program staff to review and update the MSLP Identity Theft Prevention Program. A copy of the proposed Identity Theft Prevention program is attached to this agenda item.

The newly updated program provides information on:

- Program adoption and administration,
- Definitions,
- Purpose and scope,
- Identification of red flags and the response to those red flags,
- How to prevent and mitigate identity theft, and
- Program updates.

The program was designed to meet the FTC's requirements for the "four basic elements that create a framework to deal with the threat of identity theft."

1. A program must include reasonable policies and procedures to identify the red flags of identity theft that may occur in your day-to-day operations.

2. A program must be designed to detect the red flags you've identified.

3. A program must spell out appropriate actions you'll take when you detect red flags.

4. A program must detail how you'll keep it current to reflect new threats.

The Red Flags Rule requires that an agency's board of directors approve the initial program. Based on federal guidelines, the board may oversee, develop, implement, and administer the program, or it may designate a senior employee to accomplish those tasks. Because a senior employee was not previously designated, this

item requests the CBHE approve the updated Identity Theft Prevention Program. In addition, it is recommended that the CBHE designate the DHEWD Information Security Senior Associate as the program administrator. The program administrator may report to the CBHE annually regarding the effectiveness of the program, any significant incidents of identity theft and our response, and information on any changes to the program.

RECOMMENDATION

Staff recommend that the Coordinating Board for Higher Education approve the Identify Theft Prevention Program attached to this agenda item. Staff also recommend that the Coordinating Board designate the DHEWD Information Security Senior Associate as the administrator for the program.

ATTACHMENT

- Missouri Student Loan Program Identity Theft Prevention Program

Tab 20 Attachment
Missouri Student Loan Program Identity Theft Prevention Program

Missouri Student Loan Program (MSLP) Identity Theft Prevention Program

Last CBHE Approved	10/23/2008
Last Reviewed	7/2/2021
Last Modified	7/2/2021
NIST 800-53 Compliance	PM-18, PM-19, PM-20

I. PROGRAM ADOPTION

The Missouri Department of Higher Education and Workforce Development (DHEWD) developed this Identity Theft Prevention Program ("Program") pursuant to the Federal Trade Commission's Red Flag Rule ("Rule"), 16 CFR § 681.2, which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003, 15 USC 1681 et seq. This Program was developed with oversight and approval of the DHEWD Coordinating Board

for Higher Education (CBHE). After consideration of the size and complexity of the MSLP's operations and account systems, and the nature and scope of the MSLP's activities, the CBHE determined that this Program was appropriate for the MSLP, and therefore approved this Program on October 23, 2008, effective beginning November 1, 2008.

II. DEFINITIONS

The Red Flag 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."

According to the Rule, the MSLP 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."

All of the MSLP's guaranteed student loan accounts are covered by the Rule. Under the Rule, a "covered account" is:

1. An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions. Covered accounts include credit card accounts, mortgage loans, automobile loans, margin accounts, cell phone accounts, utility accounts, checking accounts; and
2. Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation or litigation risks.

"Identifying information" is defined under the Rule as "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, unique electronic identification number, computer's Internet Protocol address, or routing code.

III. PROGRAM PURPOSE AND SCOPE

Under the Red Flag Rule, every financial institution and creditor is required to establish an "Identity Theft Prevention Program" tailored to its size and complexity, and the nature of its operation. Each program must contain reasonable policies and procedures to:

1. Identify risks that signify potentially fraudulent activity within new or existing borrower accounts;
2. Detect risks 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 borrower's personal identifiable information.

This Program applies to MSLP employees, service providers, contractors, consultants, and other third-parties.

IV. IDENTIFICATION OF RED FLAGS

In order to identify relevant red flags, the MSLP considered the types of accounts that it maintains, the methods it previously provided to open its accounts, the methods it provides to access its accounts, and its previous experiences with identity theft. The MSLP considered each of the following categories in order to identify red flags.

A. Alerts, notifications, or other warnings received from creditable sources or the borrower
B. The presentation of suspicious documents (proof of identity, photo id, etc.)
C. The presentation of suspicious personal information
D. Observing suspicious account activity or unusual use of an account

V. RESPONSE TO RED FLAGS

RED FLAG	RESPONSE
The MSLP is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person of an account opened by a person engaged in identity theft.	The MSLP places an ID Theft Flag on all potentially affected accounts. The flag halts all activity on the account.
The MSLP is notified by a reporting agency of an active duty alert.	The MSLP places a Military Duty Flag on all potentially affected accounts. The flag halts all activity on the account.
Documentation appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.	The MSLP notifies the US Department of Education's Office of the Inspector General and notates account to prevent further processing. Inspector General's Hotline Office of Inspector General U.S. Department of Education 400 Maryland Avenue, SW Washington, DC 20202-1500
Personal identifying information provided is inconsistent when compared against external information sources (NSLDS, DOLIR, etc.).	The MSLP will send a letter to the borrower advising of a discrepancy on the account and requesting the borrower provide documentation to prove their personal identifying information. In cases of a date of birth discrepancy, the borrower must provide either a birth certificate or a Real ID. Note that

	the MSLP service provider handles NSLDS data discrepancies.
Personal identifying information provided is inconsistent with other personal identifying information provided by the customer.	The MSLP will send a letter to the borrower advising of a discrepancy on the account and requesting the borrower provide documentation to prove their personal identifying information. In cases of a date of birth discrepancy, the borrower must provide either a birth certificate or a Real ID.
The Social Security number (SSN) provided is the same as that submitted by other persons.	The MSLP will immediately contact the borrower(s) and ask for identification to verify the borrowers' claim to the SSN. A pseudo SSN may be placed on the account.

VI. PREVENTING AND MITIGATING IDENTITY THEFT

In order to decrease the likelihood of identity theft occurring with respect to MSLP accounts, the MSLP will take the following steps with respect to its internal operating procedures to protect customer identifying information:

1. Ensure complete and secure destruction of paper documents and computer files containing customer information;
2. Ensure that office computers are password protected and that computer screens lock after a 15 minutes of inactivity;
3. Keep accessible work areas clear of papers containing customer information;
4. Utilize secured methods of communication (encrypted e-mail, SFTP, etc.);
5. Ensure paper and imaged documents are securely stored;
6. Promptly retrieve printed documents or use secure printing;
7. Require and keep only the kinds of customer information that are necessary for the MSLP's purposes;
8. Remediate any findings found during security assessments or audits;
9. Perform an annual risk assessment;
10. Ensure information systems are logically and physically protected from unauthorized use;
11. Provide limited access to authorized personnel;
12. Ensure mobile devices and laptops are secured from unauthorized use;

VII. PROGRAM ADMINISTRATION

A. Oversight

Responsibility for developing, implementing and updating this Program will lie with a Program Administrator (Senior Associate of Information Security). The Program Administrator will be responsible for the Program administration, for ensuring appropriate training of MSLP 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.

B. Staff Training and Report

MSLP staff shall be trained annually 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.

C. Service Provider Arrangements

The MSLP engages a guarantor service provider to perform various activities in connection with the MSLP's student loan program. As a result, in order 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 the MSLP will:

- Require that the service provider has such policies and procedures in place;
- Review such policies and procedures at least annually,
- Require the service provider to submit results of security assessments and audits, and
- Require the service provider to notify the MSLP of any identified red flags.

D. Program Reporting

Incidents discovered as a result of Red Flag investigation findings will be escalated to the appropriate level and authority and/or the Program Administrator. Upon request, a report will be made to the CBHE with regard to compliance, effectiveness, Red Flags discovered and recommendations for revisions.

VIII. PROGRAM UPDATES

The Program Administrator will review and update this Program annually to reflect changes in risks to customers and the soundness of the MSLP from identity theft. In doing so, the Program Administrator will consider the MSLP's experiences with identity theft situations, changes in identity theft methods, changes in identity theft detection and prevention methods, and changes in the MSLP'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 or present the CBHE with recommended changes and the CBHE will make a determination of whether to accept, modify, or reject those changes to the Program.