PN 3.118

FROSTBURG STATE UNIVERSITY
IDENTITY THEFT PREVENTION PROGRAM

Approved November 18, 2009

I. PURPOSE AND APPLICABILITY

This Policy describes the University's Identity Theft Prevention Program mandated by the Federal Trade Commission's Fair and Accurate Credit Transactions Act (FACT Act), which amended the Fair Credit Reporting Act (FCRA), , also known as the Red Flags Rule regulations under sections 114 and 315 of the FACT Act. This mandate requires financial institutions and creditors that hold covered accounts to develop and implement an identity theft prevention program for new and existing accounts. Institutions of higher education, whose fiscal operations fall within the Red Flag Rules, are mandated to identify, detect, prevent and mitigate instances of identity theft.

Some procedures mandated by the Red Flag Rules are also within the purview of other federal or state laws which require the securing and safeguarding of personal financial information. Accordingly, this Identity Theft Prevention Program incorporates and is in addition to institutional policies and procedures required by other federal and state laws and regulations, including, without limitation, the Family Educational Rights and Privacy Act ("FERPA"). When another University policy overlaps with the Red Flag Rules, the more specific policy will take precedence, provided that the specified safeguards meet the minimum Identity Theft Prevention Program requirements. The level of monitoring will be appropriate based upon the potential impact and probability of the risks identified, as well as the sensitivity of the information.

II. DEFINITIONS

A. "Red Flag Rules Identity Theft Prevention Program" (the "Program"): The administrative, technical, or physical safeguards the University uses to identify, detect, prevent and mitigate instances of identity theft, as required under the Federal Trade Commission's FACT Act and the Red Flag Rule regulations.

B. "Financial Institution": A state/national bank, savings & loan association, mutual savings bank, state/federal credit union or any other entity that directly or indirectly holds a transaction account belonging to a customer.

C. “Creditor”: Federal law defines a creditor as an entity that regularly extends, renews, or continues credit; any entity that regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who is involved in the decision to extend, renew, or continue credit. Where non-profit and government entities defer payment for goods or services, they are considered creditors. The federal law also includes any entity that defers payment for services rendered, such as an organization that bills at the end of the month for services rendered the previous month. For example, the University falls within the definition of creditor by participation (i) in the Federal Perkins Loan Program; (ii) as a school lender in the Direct Lending Program; (iii) in offering institutional loans to students, faculty or staff; and (iv) in offering a plan for payment of tuition throughout the semester rather than requiring full payment at the beginning of the semester.

D. “Covered Accounts”: A consumer account that involves multiple payments or transactions, such as a loan that is billed or payable monthly. This would include any type of account or payment plan that involves multiple transactions or multiple payments in arrears. A covered account is also an account for which there is a reasonably foreseeable risk of identity theft.

E. “Red Flag”: A pattern, practice or specific activity that could indicate identity theft.

F. “Collection Unit”: Any University department or unit that administers covered accounts. Collection units will be identified through procedures established under this Policy, and include, but are not limited to, the Office of Information Technology; Associate Vice President for Finance; Bursar’s Office; Financial Aid Office; Health Center, University Library and Perkins Loan.

III. RESPONSIBLE ADMINISTRATOR

A. The University’s Vice-President of Administrative and Finance, or designee, (hereinafter referred to as the “Program Officer”) is responsible for coordinating and overseeing the Program. The Program Officer shall perform these duties in conjunction with representatives from offices identified as Collection Units. Unit shall develop identity theft procedures to implement under this Program.

IV. IMPLEMENTATION

A. As required by federal law, the University’s Program has the following four components:

(i) Identification of relevant "Red Flags" and incorporation of them into the Program;
(ii) Detection of Red Flags that the Program incorporates;
(iii) Prevention and mitigation of identity theft by responding appropriately to detected Red Flags; and
(iv) Evaluation and adjustment of the Program periodically to reflect changes in risks, including periodic evaluation and adjustment of the Program based upon the results of testing and monitoring as well as changes in operations or operating systems.

B. Identification of Relevant Red Flags. The University shall consider the following risk factors in identifying relevant Red Flags for covered accounts: (i) types of covered accounts it offers or maintains; (ii) methods it provides to open its covered accounts; (iii) methods it provides to access its covered accounts; and (iv) its previous experiences with identity theft..

The University shall incorporate relevant Red Flags from sources such as: (i) incidents of identity theft that the University has experienced; (ii) methods of identity theft that the University has identified that reflect changes in identity theft risks; and (iii) applicable supervisory guidance.

The University's Program shall include Red Flags from the following categories: (i) alerts, notifications or other warnings received from consumer reporting agencies or service providers, such as fraud detection services; (ii) the presentation of suspicious documents; (iii) the presentation of suspicious personal identifying information, such as a suspicious address change; (iv) the unusual use of, or suspicious activity related to, a covered account; and (v) notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the University.

C. Detection of Red Flags. Policies and procedures shall be established to address the detection of Red Flags in connection with the opening of covered accounts and the maintenance of existing covered accounts. This shall be done by obtaining identifying information about, and verifying the identity of, a person opening a covered account, for example, using the policies and procedures regarding identification and verification set forth in the Customer Identification Program rules codified in 31 U.S. C. 5318(l) (31 CFR 103.121); and authenticating customers, monitoring transactions, and verifying the validity of change of address requests, in the case of existing covered accounts.

D. Prevention and Mitigation of Identity Theft. The Program shall provide for appropriate responses to the Red Flags the University has detected that are commensurate with the degree of risk posed. The Program will consider

aggravating factors that may heighten the risk of identity theft. Such factors include, but are not limited to, a data security incident that results in unauthorized access to a customer's account records or notice that a customer has provided information related to a covered account to someone fraudulently claiming to represent the Institution.

E. Evaluation and Adjustment of the Program. On an annual basis, the Program Officer, working with the Collection Units and responsible units and offices, shall evaluate and adjust the Program to reflect changes in risks to customers or to the safety and soundness of the University from identity theft, based on factors such as: (i) University experience with identity theft; (ii) changes in methods of identity theft; (iii) changes in methods to detect, prevent, and mitigate identity theft; (iv) changes in the types of accounts that the University offers or maintains; and (v) changes in the business arrangements of the University, including mergers, acquisitions, alliances, joint ventures and service provider arrangements.

Following the evaluation process, the Collection Units shall modify their respective identity theft prevention procedures as necessary to implement identified revisions in the Program.

Internal