Wesleyan University Identity Theft Prevention Program

APPLICATION: All "Covered Accounts" as Described Herein and all University Employees and/or Providers Working with Such Accounts
ISSUED: ***March 1, 2009***
REVISED:

I. Purpose. This Wesleyan University Identity Theft Prevention Program (the "Program") is intended to implement the requirements of Federal Trade Commission's Red Flags Rule, issued under the Fair and Accurate Credit Transactions Act of 2003 (the "Rule"). The Program is designed to detect, prevent and mitigate identity theft in connection with the opening or operation of a Covered Account.

II. Definitions.

a. A *Covered Account* means an account that the University or a third party acting for the University offers or maintains that is designed to permit multiple payments or transactions and any other account that the University offers for which there is a reasonably foreseeable risk to customers or the safety and soundness of the University with respect to identity theft. The University anticipates that Covered Accounts at the University include:

i. Refund of credit balances involving PLUS loans
ii. Refund of credit balances, without PLUS loans
iii. Student accounts
iv. Emergency loans
Service provider covered accounts may include (current provider noted)
v. Tuition Management Systems, a division of Key Bank (administers the ten month tuition payment plan)
vi. Campus Partners (administers the Perkins Loans and Wesleyan Long Term Loan repayments)
vii. Nelnet (administers the student accounts e-billing and campus-wide electronic payment system

b. *Red Flags* are patterns, practices or specific activity that indicate the possible existence of identity theft, including but not limited to those "red flags" identified on Schedule A attached hereto.

III. Program Statement. All Wesleyan University employees or providers will:
a. Take reasonable preventative measures to mitigate the risk of identity theft;

b. Monitor their involvement with all Covered Accounts to identify evidence of Red Flags; and
c. Take all reasonable remedial measures upon the identification of a Red Flag, including but not limited to the following as appropriate to the circumstances:

    i. Deny access to or freeze the Covered Account until the issue is resolved;
    ii. Contact the holder of the Covered Account as soon as possible;
    iii. Work with the Covered Account holder to immediately change passwords or other security protocols for the account; and
    iv. Notify law enforcement or other agencies or departments

IV. Program Responsibility & Oversight. The Associate Vice President for Finance (the "Program Officer") shall be responsible for implementing and updating this Program, including ensuring the appropriate training of employees and providers covered hereunder. The Program Officer will, at least annually and in conjunction with all applicable personnel, consider the University's experiences and identify any required changes to the Program and implement the same. Additionally, the Program Officer will ensure that all applicable personnel are trained in the Program.

Schedule A

Non-Exhaustive Examples of Red Flags

Fraud or similar alert	Notice of credit freeze	Notice of address discrepancy
Pattern of activity inconsistent with account history	Suspected forged, altered or inconsistent identification documents	Suspected forged, altered or inconsistent application documents
Personal identifying information is inconsistent when compared to external sources	Personal identifying information is inconsistent with other information provided by account holder	Personal identifying information is associated with known fraudulent activity
Personal identifying information is of a type commonly associated with fraudulent activity (e.g. mail drops, fictitious address)	SSN is same as that submitted by other persons	Address or phone number is same as that submitted by other persons or significant number of other persons
Applicant fails to provide all required identifying information	Request for replacement documents or information received shortly after account opening or change of address	Dormant account is suddenly used in an unprecedented way
Mail sent to account holder is returned repeatedly as undeliverable while transactions continue to occur	Notice received of unauthorized charges or transactions	Notice received from account holder or related person claiming to be a victim of identity theft