Title: Identity Theft Detection and Prevention (Red Flag) Policy; Staff

Policy Reference: By-Laws of Benedictine University

Background:

The Federal Trade Commission's Red Flags Rule, implementing Section 114 of the Fair and Accurate Credit Transactions Act of 2003, requires Universities having Covered Accounts to implement Identity Theft prevention and detection programs appropriate to the size and complexity of their operations and account systems; and the nature and scope of their activities. The Rule mandates the creation and continued administration of a program designed to detect, prevent and mitigate Identity Theft in existing Covered Accounts or the opening of new Covered Accounts.

Policy Statement:

Benedictine University's ("University") Red Flag Program ("Program") identifies and incorporates into the Program, relevant Red Flags for Covered Accounts; detects and reasonably responds to Red Flags in order to prevent and mitigate Identity Theft; and ensures the Program is updated periodically to reflect changes in risks to students from Identity Theft. Service Providers engaged to perform activities in connection with covered accounts or loans covered by the Program, are required by contract to perform in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of Identity Theft and to report detected Red Flags to the University.

The Program applies to all employee and student loans with the University and all employee and student financial accounts or payment plans for debts owed to the University that involve multiple transactions or multiple payments. The Program does not apply to financial transactions where the University is not a creditor or lender (e.g., arrangements for employee direct deposit of payroll checks, acceptance of checks or credit cards for on-campus purchases or donor gifts to the University, etc.). Neither does the Program apply to any non-financial transaction (e.g., transcript requests, requests for issuance of keys to campus offices, requests to give an employee or student access to a confidential database.)

Definitions:

- **Covered Account:** Employee or student accounts, loans and payment plans for debts owed to the University that involve multiple transactions or multiple payments and are administered by the University.
- **Identifying Information:** A name or number that may be used, alone or with other information, to identify a specific person, including: name, address, telephone number, date of birth, social security number, valid driver's license or government issued identification number, alien registration number, passport number, taxpayer identification number, student number, Internet Protocol address, or routing code.
- **Identity Theft:** Unauthorized use of the Identifying Information of another person, to commit or attempt to commit a fraud.
- **Red Flag:** Activity that indicates the possibility of Identity Theft.
- **Service Provider:** Any third party providing services, goods, assets, or facilities to the

University including contractors, sub-contractors, consultants, professional service contractors, and suppliers.

Roles and Responsibilities:

Detecting Red Flags

- In order to detect Red Flags for new or existing accounts, Benedictine University employees are responsible to:
  - Require identifying information such as name, date of birth, academic records, home address or other identification to verify the person's identity at the time of employment, enrollment, opening an account or applying for a loan;
  - Verify the person's identity by reviewing a driver's license or other government-issued photo identification at the time Bencards are issued;
  - Verify the identity of students and employees requesting account or loan information (in person, via telephone, via facsimile, via email); or attempting to conduct transactions on covered accounts;
  - 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;
  - Verify changes in banking information given for billing and payment purposes;
  - Use reasonable measures to monitor transactions on particular accounts including employee and student tuition loans, loan repayment assistance programs, tuition payment plans, payroll advances, and employee and student accounts billed monthly;
  - Require Service Providers by contract, to have reasonable policies for the detection, prevention and mitigation of Identity Theft and to report any detected red flags to the University.
  - Use appropriate diligence, and follow other University policies and procedures for any transaction outside the scope of the Program having privacy or information security implications;
- In order to detect Red Flags in a credit or background report obtained for volunteer or job applicant, Benedictine University employees are responsible to:
  - Require written verification from all applicants 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;
  - If a notice of address discrepancy is received, verify that the credit report pertains to the applicant for whom the request was made and report the confirmed address for the applicant to the consumer reporting agency.

Preventing and Mitigating Identity Theft

- In the event a Red Flag is detected, Benedictine University employees are responsible to take one or more of the following steps, depending on the degree of risk posed by the Red Flag:
  - Immediately notify their manager, Campus Safety or the Director of the Office of Institutional Compliance and Risk Management for determination of the appropriate step(s) to take;
  - Monitor the Covered Account for evidence of Identity Theft;
  - Contact the student or applicant (for whom a credit report was obtained);
  - Change passwords or other security devices that permit access to Covered Accounts;

- Not open a new Covered Account;
- Provide the student with a new student identification number;
- Notify law enforcement;
- Determine that no response is warranted under the particular circumstances.

- In order to further reduce the risk of Identity Theft, University employees are responsible to protect student identifying information by taking the following steps:
  - Avoid use of social security numbers;
  - Require only the student information necessary for University purposes.
  - Password protect office computers with access to Covered Account information;
  - Completely and securely destroy paper documents and computer files containing student account information when a decision has been made to no longer maintain such information;

Program Administration

- At least annually or as requested by the Director of the Office of Institutional Compliance and Risk Management, University managers responsible for development, implementation, and administration of the Program shall report on compliance with this Program. The report should address;
- - Significant incidents involving identity theft;
  - Management's response;
  - Recommendations for changes to the Program;
  - Service provider arrangements;
- The Director of the Office of Institutional Compliance and Risk Management is responsible to:
  - Ensure appropriate training of University staff to effectively implement the Program;
  - Review particular cases or issues of possible Identity Theft reported by University employees and determine what preventive or mitigating measures are appropriate under the circumstances;
  - Consider periodic changes to the Program.
  - Assess compliance with the Program during periodic Compliance Reviews.
- Information about the University's specific Red Flag identification, detection, and mitigation and prevention practices is limited to those employees with a need to know them. Program documents describing specific practices are considered "confidential" and should not be shared with other University employees or the public.

Contacts:

- Director of the Office of Institutional Compliance and Risk Management (630) 829-6404
- Chief Information Officer (630) 829-6449
- Dean of Students (630) 829-6006
- Director - Office of Financial Aid (630) 829-6415
- Director - Campus Safety (630) 829-1101

Additional Resources:

- ***Benedictine University Red Flags List***
- ***Faculty Handbook***
- ***Employee Handbook***

Date of Issuance: July 29, 2009
Last Revised: January 23, 2023
Department Responsible: Office of Institutional Compliance and Risk Management