BRIDGEWATER STATE UNIVERSITY POLICE DEPARTMENT
Identity Theft Prevention Policy

Purpose

This policy is adopted to comply with the Fair and Accurate Credit Transactions Act and federal regulations – promulgated at 16 CFR § 681.2 – in order to detect, prevent and mitigate identity theft by detecting identity theft red flags and by responding to such red flags in a manner that will prevent identity theft.

Definitions

Identity theft means fraud committed or attempted using the identifying information of another person without authority.

A **covered account** means:

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 savings accounts.

2. Any other account that the institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the institution or creditor from identity theft, including financial, operational, compliance, reputation or litigation risks.

A **red flag** means a pattern, practice or specific activity that indicates the possible existence of identity theft.

The Program

The Bridgewater State University Police Department has established an Identity Theft Prevention Program in an attempt to detect and prevent identity theft. The Program shall include these reasonable policies and procedures to:

1. Identify relevant red flags based on risk factors associated with the University's covered accounts.
2. Institute procedures for detecting red flags.
3. Describe the response to any red flags that are detected.
4. Create a system for regular updates to and administrative oversight of the Program.

The Program shall, as appropriate, incorporate existing policies and procedures that control reasonably foreseeable risks.

Administration of Program

1. The chief of police shall be responsible for the Bridgewater State University Police Department's development, implementation, oversight and continued administration of the Program.

2. The chief of police shall train staff, as necessary, to effectively implement the Program.

3. The chief of police shall exercise appropriate and effective oversight of service provider arrangements.

Identification of Relevant Red Flags

1. Relevant red flags may appear in the following categories:

    - Suspicious documents.
    - Suspicious personal identifying information.
    - Suspicious or unusual use of a covered account.
    - Alerts from others (identity theft victim, other law enforcement agencies).

Detection of Red Flags

This section shall address the detection of red flags in connection with the opening of covered accounts and existing covered accounts.

A. New accounts

1. As a precondition for opening a new, covered account, the department will require complete personal identifying information (i.e., full name, date of birth, address, government-issued ID, etc.).

B. Existing accounts

1. Department staff will verify validity of requests for changes of billing address.
2. Staff will verify identification before giving out any personal information.

Response

In order to prevent and mitigate the effects of identity theft, appropriate responses may include:

1. Monitoring a covered account for evidence of identity theft.
2. Changing any passwords, security codes or other security devices that permit access to a covered account.
3. Reopening a covered account with a new account number.

4. Not opening a new covered account.
5. Closing an existing covered account.
6. Beginning an investigation.
7. Determining if a response is warranted under the particular circumstances.

Updating the Program

1. The chief of police is responsible for developing, implementing, and administering and updating the Program.

Duties Regarding Address Discrepancies

The Bridgewater State University Police Department shall develop policies and procedures designed to enable the organization to form a reasonable belief that a credit report relates to the consumer for whom it was requested if the organization receives a notice from internal and/or external sources or of an address discrepancy from a nationwide consumer reporting agency indicating if the address given by the consumer differs from the address contained in the consumer report.

The Police Department may reasonably confirm that an address is accurate by any of the following means:

1. Verification of the address with the consumer.
2. Review of the authorized Bridgewater State University's records.
3. Verification of the address through third-party sources if applicable.
4. Other reasonable means.

Reviewed 3/2026