



BRAINERD PUBLIC UTILITIES

8027 Highland Scenic Rd • P.O. Box 373 • Brainerd, Minnesota 56401

Business Office: 218.829.8726 ■ **Repair Service:** 218.829.2193

www.bpu.org

Identity Theft Prevention Program Procedures

BPU_POL_2008-14

Latest Revision/Effective Date: September 29, 2026

Original Adoption Date: November 25, 2008

I. Purpose

To establish an Identity Theft Prevention Program that detects, prevents, and mitigates identity theft in connection with new and existing utility accounts. The intended outcome is to safeguard customer identifying information and protect the financial integrity of the utility.

II. Scope

This policy applies to all current and prospective customer accounts maintained by Brainerd Public Utilities (BPU). It governs all methods of account opening and access to account information, including in-person, telephone, fax, and online channels. All BPU employees must comply with this policy, with responsibility placed on employees who have access to sensitive customer information.

III. Definitions

Account: A customer record maintained by BPU for the provision and billing of electric, water, or wastewater utility services to specific premises, including accounts in the process of being opened.

Consumer Report: A report issued by a consumer reporting agency containing information about an individual's credit history, identity, or other characteristics, which may be used in evaluating an application for service.

Consumer Reporting Agency: A business that compiles and provides consumer reports, such as a national credit bureau.

Customer: Any individual, business, property owner, tenant, estate, or legal entity that has established or is applying to establish an account with BPU.

Fraudulent Account: An account opened or maintained using false, stolen, or unauthorized identifying information.

Identifying Information: Any name or number that may be used, alone or together with other information, to identify a specific person, including name, address, telephone number, Social Security number, date of birth, driver's license or government-issued identification number, and bank account or payment card information.

Identity Theft: A fraud committed or attempted using the identifying information of another person without authority.

Identity Theft Prevention Program: The written program adopted by BPU to identify, detect, and respond to red flags and to prevent and mitigate identity theft in connection with new and existing accounts.

Red Flag: A pattern, practice, or specific activity that indicates the possible existence of identity theft.

Risk Assessment: An internal evaluation of the methods used to open accounts and access account information, conducted to determine the likelihood that a fraudulent account could be opened or an existing account manipulated.

Security Deposit: A security amount required by BPU as a condition of service, established in accordance with the BPU fee schedule.

IV. Policy Statement

BPU is committed to protecting customer personal information and mitigating the risk of identity theft.

BPU will administer an Identity Theft Prevention Program based on an assessment of the identity theft risks associated with the accounts it maintains and the methods used to open and access them. The program alerts BPU employees to red flags indicating an account may have been opened or accessed using false information, protects against the establishment of fraudulent accounts, provides methods to verify that existing accounts were not opened using false information, and establishes measures to respond when such activity is detected.

BPU will verify customer identity before opening an account, releasing account information, or processing changes to billing address or banking information. If a customer refuses to provide the information necessary to verify their identity, BPU will require an additional security deposit as a condition of service.

V. Procedures

A. Risk Assessment

BPU has conducted an internal risk assessment to evaluate how at risk the current procedures are at allowing customers to create a fraudulent account and evaluate if current (existing) accounts are being manipulated. This risk assessment evaluated how new accounts were opened and the methods used to access the account information. Using the following information, BPU was able to identify the following red flags that were appropriate to prevent identity theft.

- New accounts opened in person
- New accounts opened via telephone
- New accounts opened via fax

- Existing account information accessed in person
- Existing account information accessed via telephone
- Existing account information accessed via web site

B. Detection (Red Flags)

BPU adopts the following red flags to detect potential fraud. These are not intended to be all-inclusive and other suspicious activity may be investigated as necessary.

1. New Customers

- Fraud or active duty alerts included with consumer reports
- Notice of credit freeze provided by consumer reporting agency
- Notice of address discrepancy provided by consumer reporting agency
- Inconsistent activity patterns indicated by consumer reports such as
 - Recent and significant increase in volume of inquiries
 - Unusual number of recent credit applications
 - A material change in use of credit
 - Accounts closed for cause or abuse
- Identification documents appear to be altered
- Photo and physical description do not match appearance of applicant
- Other information is inconsistent with information provided by applicant
- Other information provided by applicant is inconsistent with information on file
- Application appears altered or destroyed and reassembled
- Personal information provided by applicant does not match other sources of information (e.g. credit reports, SSN not issued or listed as deceased)
- Lack of correlation between the SSN range and date of birth
- Information provided is associated with known fraudulent activity (e.g. address or phone number provided is same as that of a fraudulent application)
- Information commonly associated with fraudulent activity is provided by applicant (e.g. address that is a mail drop or prison, non-working phone number or associated with answering service/pager)
- SSN, address, or telephone number is the same as that of other customer at BPU
- Customer fails to provide all information that is requested on application
- Personal information provided is inconsistent with information on file for a customer
- Applicant cannot provide information requested beyond what could commonly be found in a purse or wallet
- Identity theft is reported or discovered

2. Existing Customers

- Verify the identification of customers if they request information (in person, via telephone, via fax, via email)

- Verify the validity of requests to change billing address
- Verify changes in banking information given for billing and payment purpose

If a customer refuses to give necessary information, an additional security deposit will be required.

C. Response Protocols

Any employee who suspects fraud or detects a red flag will implement the following responses as applicable:

1. Request additional verification documentation from the applicant.
2. Deny account opening or immediately close the active account.
3. Halt all collection attempts against the affected account and notify authorities.
4. Report the activity internally to the Business Office Supervisor or Finance Manager.
5. Notify law enforcement via the Brainerd Police Department regarding attempted or actual identity theft.

D. Personal Information Security Procedures

The following measures are not required by the Federal Trade Commission's Identity Theft Red Flags Rule, but BPU adopts them to further protect customer information.

- Paper documents, files, and electronic media containing secure information will be stored in locked file cabinets.
- Files containing personally identifiable information are kept in locked file cabinets except when an employee is working on the file.
- Employees will not leave sensitive papers on their desks when they are away from their workstations.
- Employees store files when leaving their work area.
- Employees log off their computers when leaving their work areas at the end of the day.
- Employees lock file cabinets when leaving their work areas at the end of the day.
- Any sensitive information shipped using outside carriers or contractors will be encrypted.
- Any sensitive information shipped will be shipped using a shipping service that allows tracking of the delivery of this information.
- No visitor will be given any entry codes or allowed unescorted access to the BPU office.
- Computer passwords will be required.
- Passwords will not be shared or posted near workstations.

- When installing new software, immediately change vendor-supplied default passwords to a more secure strong password.
- Ensure that BPU's website is secure or provide clear notice that the website is not secure.
- Anti-virus and anti-spyware programs will be run on individual computers and on servers daily.
- The use of laptops is restricted to those employees who need them to perform their jobs.
- Laptop users will not store sensitive information on their laptops.
- Employees are required to notify the IT Department, finance manager, or their supervisor immediately if there is a potential security breach, such as a lost or stolen laptop.
- Any wireless network in use is secured.
- The computer network will have a firewall where BPU's network connects to the Internet.
- Check references or do background checks before hiring employees who will have access to sensitive data.
- New employees sign an agreement to follow BPU's confidentiality and security standards for handling sensitive data.
- Access to customer's personal identifying information is limited to employees with a "need to know."
- Implement a regular schedule of employee training.
- Employees will be alert to attempts at phone phishing.
- Employees who violate security policy are subjected to discipline, up to, and including, dismissal.
- Service providers notify BPU of any security incidents they experience, even if the incidents may not have led to an actual compromise of BPU's data.
- Paper records will be shredded before being placed into the trash.
- Any data storage media will be disposed of by shredding, punching holes in, or incineration.

VI. Roles and Responsibilities

Finance Manager (Program Administrator): Manages program administration, ensures staff training, reviews operational red flag reports, determines mitigation paths, and processes periodic updates. Evaluates changing risks at least once a year.

Business Office Supervisor / Supervisors: Serves as the internal reporting pipeline for staff discovering active red flags and potential security breaches.

BPU Staff / Employees: Obligated to follow confidentiality standards, complete required training, remain alert to phone phishing, and strictly enforce identity verification rules.

VII. Compliance and References

- Federal Trade Commission's Red Flags Rule (16 C.F.R. § 681.2).
- Section 114 of the Fair and Accurate Credit Transactions Act of 2003.
- Background Checks: Mandatory background and reference screenings are required for all prospective employees handling sensitive data.
- Enforcement: Violations of this policy will result in disciplinary action up to and including employment dismissal.

VIII. Associated Forms and Attachments

- New Customer Identity Verification Forms.
- New Employee Confidentiality & Security Standards Agreement.
- Account Address/Banking Change Validation Forms.

IX. Review and Update Schedule

This policy is reviewed at least annually by the Finance Manager. The evaluation reviews local experiences with identity theft, shifting fraud methodologies, new detection equipment, and evolving account structures or business vendor arrangements.

X. Approval and Authority

The Brainerd Public Utilities Commission approved this policy on September 29, 2026.