BRAINERD PUBLIC UTILITIES
POLICY 2008-14
Identity Theft Prevention Program Procedures
Adopted 11/25/08

This program is intended to identify red flags, pursuant to the Federal Trade Commission's Red Flags Rule which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003 (16 C.F.R. § 681.2), that will alert Brainerd Public Utilities (BPU) employees when new or existing accounts are opened using false information; protect against the establishment of false accounts; methods to ensure existing accounts were not opened using false information; and measures to respond to such events.

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

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.

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

<u>Existing Customers</u>

- 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 purposes

IF A CUSTOMER REFUSES TO GIVE NECESSARY INFORMATION AN ADDITIONAL SECURITY DEPOSIT WILL BE REQUIRED.

Reponse to Red Flags

Any employee that may suspect fraud or detect a red flag will implement the following response as applicable.

- Ask applicant for additional documentation
- Any BPU employee who becomes aware of a suspected or actual fraudulent use of a customer or potential customer's identity must notify the Accounting Supervisor or Finance Director.
- Notify law enforcement - BPU will notify the Brainerd Police Department of any attempted or actual identity theft.
- Do not open the account
- Close the account
- Do not attempt to collect against the account, but notify authorities

Personal Information Security Procedures

The following suggestions are not part of or required by the Federal Trade Commission's "Identity Theft Red Flags Rule" but BPU will also adopt the following additional security procedures to further protect consumer 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 out 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 superintendent, finance director, 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 identify 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.

IDENTITY THEFT PREVENTION PROGRAM UPDATES

The Identity Theft Program will be periodically reviewed and updated to reflect changes in risks to BPU customers and the reliability of BPU from identity theft. At least once a year, BPU's Finance Director will consider BPU's experiences with any identity theft situation(s) that have occurred, changes in identity theft methods, changes in identity theft detection and prevention methods, changes in types of accounts BPU maintains and changes in BPU's business arrangements with other entities. After considering these factors, the Finance Director will determine whether changes to the identity theft program, including the listing of red flags, are warranted. If warranted, the Finance Director will update the Identity Theft Program or present the BPU Commission with his recommended changes and the BPU Commission will make a determination of whether to accept, modify, or reject those changes.

Responsibility for developing, implementing, and updating this program lies with an Identity Theft Committee for BPU. The Committee will consist of the Finance Director, Accounting Supervisor, and Information Technology Supervisor. The Finance Director will be responsible for the program administration, ensuring appropriate training of BPU staff, review any staff reports regarding the detection of red flags and the steps for preventing and mitigating identity theft, determine which steps of prevention and mitigation should be taken in particular circumstances, and considering periodic changes to the program.