Bristol Tennessee Essential Services

IDENTITY THEFT PREVENTION POLICY

Subject: Identity Theft Prevention Program for Bristol Tennessee Essential Services

Purpose: The creation and implementation of an Identity Theft Prevention Program at Bristol Tennessee Essential Services (BTES) will help identify, detect, mitigate and update Red Flags that signal the possibility of identity theft in connection with the opening of an account or any existing account.

Effective Date: 06/01/10
Revised Date: 07/7/21

TABLE OF CONTENTS

PART 1
DEFINITIONS

1. For purposes of this Policy, the term *"Account"* means an account that BTES offers or maintains, primarily for personal, family, household or business purposes, that involves or is designed to permit multiple payments or transactions **and** any other account that BTES offers or maintains for which there is a reasonably foreseeable risk to customers or the safety and soundness of BTES from identity theft including financial, operational, compliance, reputation or litigation risks.

2. For purposes of this Policy, the term *"Identity Theft"* means a fraud committed or attempted using the identifying information of another person without authority.

3. For purposes of this Policy, the term *"Red Flag"* means a pattern, practice or specific activity that indicates the possible existence of identity theft. Part 3 provides a specific description of which Red Flags are applicable to this policy.

PART 2
INCORPORATION OF EXISTING POLICY AND PROCEDURE

The Identify Theft Prevention Policy is incorporated in processes (available in SMART) already in effect at BTES and will continue to operate in conjunction with this policy to achieve its stated purpose. Examples of these processes include but are not limited to:

New Electric Connect Process

Bank Draft Process

Online Customer Portal Process

PART 3
IDENTIFICATION OF RELEVANT RED FLAGS

After careful examination of our accounts, including the methods by which we open and access them and past experience with identity theft, the following events/occurrences reasonably indicate the potential for identity theft and should be considered "Red Flags" for purposes of this policy:

A. Alerts, notifications or other warnings received from consumer reporting agencies or service providers, such as fraud detections services. For the purposes of this policy, BTES will be utilizing the ONLINE Utility Exchange as their service provider to identify the "Red Flags" listed below:

1. A fraud or active duty alert is included with a consumer report.

2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.

3. A consumer reporting agency provides a notice of address discrepancy (See Part 6).

4. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:

    a. A recent and significant increase in the volume of inquiries;
    b. An unusual number of recently established credit relationships;
    c. A material change in the use of credit, especially with respect to recently established credit relationships; or
    d. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

B. The presentation of suspicious documents, such as:

5. Documents provided for identification appear to have been altered or forged.

6. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.

7. Other information on the identification is not consistent with information provided by the person opening a new account or customer presenting the identification.

8. Other information on the identification is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check.

9. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

C. The presentation of suspicious personal identifying information, such as suspicious address changes:

10. Personal identifying information provided is inconsistent when compared against external information sources used by BTES. For example:

    a. The address does not match any address in the consumer report; or
    b. The Social Security Number (SSN) has not been issued or is listed on the Social Security Administration's Death Master File.

11. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.

12. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by BTES. For example:

    a. The address on an application is the same as the address provided on a fraudulent application; or
    b. The phone number on an application is the same as the number provided on a fraudulent application.

13. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources. For example:

    a. The address on an application is fictitious, a mail drop or a prison; or
    b. The phone number is invalid or is associated with a pager or answering service.

14. The SSN provided is the same as that submitted by other persons opening an account or other customers.

15. The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.

16. The person opening the account or the customer fails to provide all required personal identifying information on an application or, in response to notification that the application is incomplete, the customer fails to provide the required personal identifying information.

17. Personal identifying information provided is not consistent with personal identifying information that is on file with BTES.

18. If BTES uses challenge questions, the person opening the account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

D. The unusual use of, or other suspicious activity related to, an account:

19. A new credit account is used in a manner commonly associated with known patterns of fraud. For example:

    a. The customer fails to make the first payment or makes an initial payment but no subsequent payments.

20. An account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:

    a. Nonpayment when there is no history of late or missed payments;
    b. A material increase in the use of available credit;
    c. A material change in purchasing or spending patterns;
    d. A material change in electronic fund transfer patterns in connection with a deposit account; or
    e. An overpayment followed by a refund request or inconsistent payments and/or multiple returned items.

21. A request is made for a refund for a payment or overpayment on an active account.

22. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's account.

23. BTES is notified that the customer is not receiving account statements.

24. BTES is notified of unauthorized charges or transactions in connection with a customer's account.

E. Notice from customers, victims of identity theft, law enforcement authorities or other persons regarding possible identity theft in connection with accounts held by BTES:

25. BTES is notified by a customer, a victim of identity theft, a law enforcement authority or any other person that it has opened a fraudulent account for a person engaged in identity theft.

PART 4
DETECTION, PREVENTION AND MITIGATION

A. Detection

In an effort to ensure proper detection of any Red Flags, all customers (consumers) must provide at least the following information/documentation before any new account will be opened:

Residential Customers

1. Full name

2. Date of birth (individual)

3. Address:
   a. Residential
   b. For an individual who does not have a residential mailing receptacle at their street address
      i. United States Post Office (PO) box number
      ii. Army Post Office (APO) box number
      iii. Fleet Post Office (FPO) box number
      iv. Residential street address of next of kin or of another contact individual

4. Two forms of identification, which shall be: (Primary) State or U.S. Government issued photo ID and (Secondary) Social Security Card, Credit/Debit Card, Employee ID, Student ID, etc.

5. Identification number, which shall be: (i) For a U.S. person, a social security number; or (ii) For a non-U.S. person, one or more of the following: a taxpayer identification number; passport number and country of issuance; alien identification card number; or number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard.

Business Customers

1. Business Name

2. Address:
   a. Business street address
   b. For a business who does not have a business mailing receptacle at their street address
      i. United States Post Office (PO) box number
      ii. Army Post Office (APO) box number

iii. Fleet Post Office (FPO) box number
iv. Business street address of another contact individual

c. For a person other than an individual (such as a corporation, partnership, or trust)
i. A principal place of business, local office or other physical location

3. Two forms of identification for the Primary authorized contact, which shall be: (Primary) State or U.S. Government issued photo ID and (Secondary) Social Security Card, Credit/Debit Card, Employee ID, Student ID, etc. One form of identification for the Secondary authorized contact(s) which shall be State or U.S. Government issued photo ID.

4. Identification number, which shall be: (i) For a sole proprietorship, a social security number; or (ii) For a partnership, LLC, Corporation or other business type, on: a taxpayer identification number.

For any account holder of an account for which the above information is not already on file at BTES, the customer will be contacted within a reasonable period of time after discovering the missing information to obtain the necessary information.

To assist with detection of Red Flags, BTES will implement the appropriate computer programs tailored to BTES' business needs to help authenticate customers, monitor transactions and change of address requests. ONLINE Utility Exchange is being used and BTES' continued use thereof is incorporated and made part of this policy.

B. Preventing and Mitigating Identity Theft

In the event a Red Flag is detected, BTES is committed to preventing the occurrence of identity theft and taking the appropriate steps to mitigate any harm caused thereby. In order to respond appropriately to the detection of a Red Flag, BTES shall consider any aggravating circumstance(s) that may heighten the risk of identity theft. After assessing the degree of risk posed, BTES will respond to the Red Flag in an appropriate manner, which may include:

1. Monitoring an account for evidence of identity theft;
2. Contacting the customer;
3. Changing any passwords, security codes or other security devices that permit access to an account;
4. Reopening an account with a new account number;
5. Not opening a new account;
6. Closing an existing account;
7. Not attempting to collect on an account or not selling an account to a debt collector;
8. Notifying law enforcement; or
9. Determining that no response is warranted under the particular circumstances.

In an effort to mitigate the damage caused by identity theft, the following program/software is being used, and BTES' continued use thereof is incorporated and made part of this policy: ONLINE Utility Exchange.

For the protection of our customers, all service providers hired by BTES to perform any activity in connection with any account must also take appropriate steps to prevent identity theft. To this end, BTES will only contract with service providers that have implemented and follow a similar identity theft prevention policy.

PART 5
PROGRAM UPDATES

BTES is committed to maintaining an Identity Theft Prevention Policy that is current with the ever-changing crime of identity theft. To that end, BTES will reassess this policy on a periodic basis, at least annually. In reassessing this policy, BTES will add/delete Red Flags in Part 3, as necessary, to reflect changes in risks to customers or to the safety and soundness of BTES from identity theft. The determination to make changes to this policy will be within the discretion of the responsible parties, identified in Part 7 of this policy, but after careful consideration of the following:

1. BTES' past experience(s) with identity theft;

2. Changes in methods of identity theft;

3. Changes in methods to detect, prevent and mitigate identity theft;

4. Changes in the types of accounts that BTES offers or maintains; and

5. Changes in the business arrangements of BTES including mergers, acquisitions, alliances, joint ventures and service provider arrangements.

PART 6
ADDITIONAL LEGAL REQUIREMENTS (IF NECESSARY)

A. Consumer Addresses

1. Address Confirmation

BTES shall furnish the consumer's address that BTES has reasonably confirmed is accurate to consumer reporting agencies as part of the information that BTES regularly furnishes for the reporting period in which BTES establishes a relationship with the consumer. In an effort to ensure that BTES maintains accurate address information for its consumers and to ensure BTES provides accurate address information of our consumers to reporting agencies, at least one of the following steps must be taken prior to providing the consumer's address to the consumer reporting agency:

a) Verify the address on file with the consumer;
b) Confirm the address being sent to the consumer reporting agency matches the address BTES has on file for that particular consumer;
c) Compare the address with information received from any third-party source; or
d) Verify by other means that are reasonably available at the time.

2. Address Discrepancies

Because BTES is a user of consumer reports, at least one of the following steps must be taken when BTES receives notice from any consumer reporting agency that a substantial difference exists between the address for the consumer that BTES provided and the address(es) in the consumer reporting agency's file for that particular consumer:

a) Compare the differing address with BTES' file by either (1) confirming that the address information provided by BTES to the consumer reporting agency is the same information BTES obtains and uses to verify the consumer's identity in accordance with the requirements of the Customer Information Program (CIP) rules 31 USC 5318 and 31 CFR 103.121; or (2) comparing the differing addresses with BTES' records and files including applications, change of address notifications, other customer account records or retained CIP documentation; or (3) comparing the differing addresses with information BTES may have received from a third-party source; or

b) Verify the information in the consumer report provided by the consumer reporting agency with the consumer.

B. Other requirements should be addressed below based on entity type

Examples:

(a) For financial institutions and creditors that are subject to 31 USC. 5318(g), filing a Suspicious Activity Report in accordance with applicable law and regulation;

(b) Implementing any requirements under 15 USC. 1681c(h) regarding the circumstances under which credit may be extended when the financial institution or creditor detects a fraud or active duty alert;

(c) Implementing any requirements for furnishers of information to consumer reporting agencies under 15 USC. 1681s-2, for example, to correct or update inaccurate or incomplete information, and to not report information that the furnisher has reasonable cause to believe is inaccurate; and

(d) Complying with the prohibitions in 15 U.S.C. l681m on the sale, transfer and placement for collection of certain debts resulting from identity theft.

DISCLAIMER: There may be additional requirements than the examples provided above. However, the above examples are not intended to be an exhaustive list.

PART 7
ADMINISTRATION

By signing below, I, Lola McVey, Director of Accounting and Finance for Bristol Tennessee Essential Services, acknowledge that I will be responsible for overseeing the implementation, management and updating of this new policy[1] and shall have the following responsibilities:

1. Assign specific responsibility for the Program's implementation, including appropriate training for staff;

    - At least annually, the assigned person/staff must report to the Director of Accounting and Finance and provide an update on the policy's effectiveness, any service provider arrangements, significant incidents involving identity theft and BTES' response and recommendations for ways to improve the program.

2. Review reports prepared by staff to ensure that BTES remains compliant with its legal responsibility to maintain an Identity Theft Prevention Program;

3. Approve material changes to this program as necessary to address changing identity theft risks; and

4. Present amended policy to the Board of Directors to be approved annually.

_____	_____	_____	____
Name(s)	Title	Authorized Signature(s)	Date

[1] Rules require oversight by the board of directors, an appropriate committee of the board or a designated employee of **senior management.**

PART 8
POLICY APPROVAL

This Identity Theft Prevention Program is hereby approved as a Policy of Bristol Tennessee Essential Services in August 2021, as authorized by the Board of Directors.

_____	_____	_____	____
Name(s)	Title	Authorized Signature(s)	Date

434691.1