WILLIAMS TOWNSHIP BOARD OF SUPERVISORS

RESOLUTION READOPTING AN IDENTITY THEFT PREVENTION PROGRAM POLICY

SUBJECT: WILLIAMS TOWNSHIP IDENTITY THEFT PREVENTION PROGRAM

RESOLUTION 2024-3

WHEREAS, the Board of Supervisors of the Williams Township is aware of the "Red Flag Rule" issued by the Federal Reserve System, the Federal Deposit Insurance Corporation, the Federal Trade Commission, the Office of the Controller of the Currency and the Office of Thrift Supervision; and

WHEREAS, the Board of Supervisors of Williams Township readopted an Identity Theft Prevention Program on January 3, 2023 by Resolution No. 2021-02; and

WHEREAS, the Township Manager has reviewed and updated the current policy and has recommended readopting it.

BE IT RESOLVED, by the Board of Supervisors of the Williams Township that the attached Identity Theft Prevention Program is adopted by the Township and shall be effective immediately.

SO RESOLVED AND ENACTED by the Board of Supervisors of Williams Township this 2nd day of January, A.D. 2024.

WILLIAMS TOWNSHIP
BOARD OF SUPERVISORS

ATTEST:

Hannah Warner

Hannah Warner, Township Secretary

George Washburn

RJ Abert

Raymond Abert

N. Michael Bryant

Identity Theft Prevention Program

For

Williams Township

655 Cider Press Road

Easton, PA 18042

January 2, 2024

Williams Township Identity Theft Prevention Program

This Program is intended to identify red flags that will alert our 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.

Contact Information:

The Senior Management Person responsible for this program is:

Name: Melody Ernst, Manager

Title: Township Manager

Phone number: 610-258-6088

The Governing Body Members of the Township are:

1. George Washburn

2. Raymond Abert

3. N. Michael Bryant

Risk Assessment

The Township 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 this information the Township was able to identify red flags that were appropriate to prevent identity theft. Add or delete items as applicable:

- □ New accounts opened via mail
- □ New accounts opened via fax
- □ Account information accessed In Person
- □ Account information accessed via Telephone (Person)

Detection (Red Flags)

The Township 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. Add or delete items as applicable:

- □ 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
- □ 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)
- □ Address, or telephone number is the same as that of other customer at utility
- □ Customer fails to provide all information requested
- □ 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

Response

Any employee that may suspect fraud or detect a red flag will implement the following response as applicable. All detections or suspicious red flags shall be reported to the senior management official. Add or delete items as applicable:

- □ Ask applicant for additional documentation

- □ Notify internal manager: Any Township employee who becomes aware of a suspected or actual fraudulent use of a customer or potential customers identity must notify Melody Ernst
- □ Notify law enforcement: The Township will notify State Police of any attempted or actual identity theft
- □ Do not attempt to collect against the account but notify authorities
- □ Use contact information to contact customer

Personal Information Security Procedures

The Township adopts the following security procedures.

1. Employees will not leave sensitive papers out on their desks when they are away from their workstations.

2. All accounts will have a driver's license identification number, or a state issued identification card number, or a passport number selected by the customer which the customer will need to provide before any information is given out over the phone or via any other electronic communication or where the customer cannot give or provide a photo identification.

3. Employees log off their QuickBooks Program when leaving their work areas.

4. No visitor will be given any entry codes or allowed unescorted access to the office.

5. Anti-virus and anti-spyware programs will be run on individual computers and on servers daily.

6. Access to offsite storage facilities is limited to employees with a legitimate business need.

7. The computer network will have a firewall where your network connects to the internet.

8. Check references or do background checks before hiring employees who will have access to sensitive data.

9. Access to customer's personal identity information is limited to employees with a "need to know".

10. Paper records will be shredded before being placed into the trash.

11. To open a new account, a customer will be required to provide complete contact information including, mail, telephone, cell phone and e-mail where applicable as well as supply a photo Identification card which will be scanned into the Township's computer and maintained with the account information.

12. Passwords will not be shared or posted near workstations.

13. Computer passwords will be required.

14. Usernames and passwords will be different.

15. The use of laptops is restricted to those employees who need them to perform their jobs.

16. Laptops are stored in a secure place.

17. Laptop users will not store sensitive information on their laptops.

18. Employees never leave a laptop visible in a car, at a hotel luggage stand, or packed in checked luggage.

19. If a laptop must be left in a vehicle, it is locked in a trunk.

20. New employees sign an agreement to follow your company's confidentiality and security standards for handling sensitive data.

21. Procedures exist for making sure that workers who leave your employ or transfer to another part of the company no longer have access to sensitive information.

22. Employees will be alert to attempts at phone phishing.

23. Employees are required to notify the Township manager immediately if there is a potential security breach, such as a lost or stolen laptop.

24. Employees who violate security policy are subjected to discipline, up to, and including, dismissal.

25. Service providers notify you of any security incidents they experience, even if the incidents may not have led to an actual compromise of our data.

26. Any data storage media will be disposed of by shredding, punching holes in, or incineration.

27. Outside contractors' access to sensitive information should be carefully controlled and locks and passwords changed if relationships change.

28. Change locks and passwords with employee turnovers.

29. No paper files shall be maintained or kept.

30. When an account is closed, all records related to the account shall only be kept if required by the Pennsylvania Historical and Museum Commission; otherwise the records of the closed account shall be destroyed.

Identity Theft Prevention Program Review and Approval

This plan has been reviewed and adopted by the Township's Board of Supervisors. Appropriate employees have been trained on the contents and procedures of this Identity Theft Prevention Program.

Signatures:

1. Date 01/02/2024
George Washburn

2. RJ Abert Date 01/02/2024
Raymond Abert

3. Date 01/02/2024
N. Michael Bryant

A report will be prepared annually and submitted to the above-named senior management or governing body to include matter related to the program, the effectiveness of the policies and procedures, the oversight and effectiveness of any third-party billing and account establishment entities, a summary of any identify theft incidents and the response to the incident, and recommendations for substantial changes to the program, if any.