SPRING-BENNER-WALKER JOINT AUTHORITY

REGULAR MEETING
April 14, 2014

ATTENDANCE:

AUTHORITY MEMBERS:	**Spring**	Gregg Heny
		Jason Scott
		Ted Onufrak
		Dondi Smeltzer
	Benner	Dan Hoffman
		William Hughes
		Timothy Miller
	Walker	Dennis McDowell
		Joseph Swanderski

GUEST: None Present

EXECUTIVE DIRECTOR: N. Warren Miller

CONSULTING SOLICITOR: Robert Mix, Esq.

EMPLOYEES: Tasha Dutton

CALL TO ORDER:

The April 14, 2014, Regular Meeting of the Spring-Benner-Walker Joint Authority was called to order at 7:00 P.M. by Timothy Miller, Chairman. Mr. T. Miller thanked everyone for attending and stated that the meeting would be recorded for transcription.

ROLL CALL:

William Hughes, Secretary, took Roll Call, recording nine members present. Mr. T. Miller, Chairman, noted that with a quorum present, the Spring-Benner-Walker Joint Authority was permitted to conduct business under the laws of Pennsylvania.

PLEDGE OF ALLEGIANCE:

Mr. T. Miller, Chairman, led the Board members and Employees in the Pledge of Allegiance.

Mr. Onufrak entered the meeting at 7:01 p.m.

APPROVAL OF MEETING MINUTES:

Mr. Hoffman moved, seconded by Mr. Smeltzer to approve the Minutes of the March 24, 2014 Regular Meeting as presented. 9 ayes, 0 nays. **The motion carried.**

CORRESPONDENCE:

Jersey Shore State Bank – We received a letter from Craig Russell, Regional President, stating that the interest rate for our bank accounts at Jersey Shore State Bank will be 0.25% effective April 1, 2014.

In-Home Sewer Inspection Program Packet – The Board members were provided copies of the presentation that Mr. W. Miller and Mrs. Gill offered at the PA Rural Water Conference in State College. The topic discussed was "How to Develop and Implement an In-Home Sewer Inspection Program". Mr. W. Miller stated that the presentation went well and he feels that many will benefit from the information provided. Mr. T. Miller congratulated Mr. W. Miller and Mrs. Gill for their work.

APPROVAL OF PAYMENTS:

Approval of Requisitions:

Revenue Fund Requisition 2012-30 – Mr. T. Miller asked if there were any questions regarding the presentation of Revenue Fund Requisition #2012-30. Mr. Hoffman questioned the payment of $12,985.31 to Capital Blue Cross. Mr. Hoffman wanted to confirm what was covered and the duration of the coverage. Mr. W. Miller explained that this payment was for the month of April and that it covers health, vision and prescription. **Mr. Swanderski moved, seconded by Mr. McDowell to approve Revenue Requisition 2012-30 payable to SBWJA in the amount of $65,596.93.** 9 ayes, 0 nays. **The motion carried.**

GUEST: There were no Guests present for the meeting.

EXECUTIVE DIRECTOR'S REPORT:

Chapter 94 Report - Mr. W. Miller informed the Board that he received a telephone call from Rob Everett of PA DEP wanting to discuss the Authority's 2013 Chapter 94 Report. Mr. Everett discussed our plan to possibly install an equalization tank at the Zion Ridge Pump Station to accommodate future growth in Walker Township. It was also noted that Mr. Everett indicated he was pleased with the Authority's work and low wet weather flows.

Rockview Billing – Our auditors from ParenteBeard, LLC recommended that the Authority consider making a change to the Rockview billing. The auditors stated that a portion of the Rockview bill is currently calculated based on the employee's net wages; however, it should be calculated using gross wages. These changes will result in additional income for the Authority. Mr. W. Miller stated that this has been the Authority's billing practice prior to the current employees. Mrs. Gill will make changes to the next quarterly bill to Rockview.

Radio Advertisement – Penn State Radio has contacted the Authority for a $900.00 donation. The donation would be to sponsor a radio advertisement that encourages students not to drink and drive. This advertisement would air for approximately 2 weeks.

SOLICITOR'S REPORT:

Graystone Court – Mr. Mix asked if the developer, Jeff Long, for Graystone Court has contacted the Authority regarding the Board's decision on a reduced user fee. Mr. W. Miller stated that Mr. Long previously indicated that he would like to attend a meeting in April to discuss this matter with the Board.

OLD BUSINESS:

Rosewood Cove – Mr. Smeltzer asked if the as-builts for Rosewood Cove have been completed and approved. The Authority received updated prints last Thursday; however, they will need to be re-evaluated.

NEW BUSINESS:

Identity Theft Prevention Program – Mr. T. Miller presented the Identity Theft Prevention Program Compliance Model to the Board for comment. 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. This Program is updated and approved on a yearly basis. Mr. T. Miller asked if there were any changes to the language of the document from last year. Mr. W. Miller stated that there were no changes to the document. **Mr. Heny moved, seconded by Mr. Smeltzer to approve the Identity Theft Prevention Program as presented for discussion and made a part of these official Minutes.** 9 ayes, 0 nays. **The motion carried.**

Radio Advertisement – Mr. T. Miller asked if there were any questions regarding the donation to Penn State Radio. The Board discussed the donation; however, decided that they were not interested in participating.

ADJOURNMENT:

Mr. Hoffman moved, seconded by Mr. McDowell to adjourn the meeting at 7:37 p.m. 9 ayes, 0 nays. **The motion carried.**

Respectfully submitted,

William Hughes, Secretary

Tasha L. Dutton, Recording Secretary

CC: Benner Township_____
Spring Township _____ > 4/21/14 mo
Walker Township_____

Identity Theft Prevention Program

For

SPRING – BENNER – WALKER JOINT AUTHORITY

170 Irish Hollow Road

Bellefonte, PA 16823

April 14, 2014

Spring – Benner – Walker Joint Authority 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: N. Warren Miller
Title: Executive Director
Phone number: 814-355-4778

The Governing Board Members of the Utility are:

1. Timothy Miller, Chairman
2. Dennis McDowell, Vice Chairman
3. Ted Onufrak, Treasurer
4. Gregg Heny, Assistant Treasurer
5. William Hughes, Secretary
6. Dondi Smeltzer, Assistant Secretary
7. Dan Hoffman
8. Joseph G. Swanderski
9. Jason Scott

Risk Assessment

The Spring Benner Walker Joint Authority 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 utility was able to identify red flags that were appropriate to prevent identity theft.

✓New accounts opened In Person
✓Account information accessed In Person

Detection (Red Flags)

The Spring Benner Walker Joint Authority 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.

✓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 report 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, SS# not issued or listed as deceased)
✓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)
✓ SS#, address, or telephone # 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.

✓Ask applicant for additional documentation
✓Notify internal manager: Any utility employee who becomes aware of a suspected or actual fraudulent use of a customer or potential customers identity must notify the Executive Director.
✓Notify law enforcement: The utility will notify the PA State Police at Rockview of any attempted or actual identity theft.
✓Do not open the account
✓Close the account

Personal Information Security Procedures

The Spring Benner Walker Joint Authority adopts the following security procedures:

1. Files containing personally identifiable information are kept in a locked file cabinet except when an employee is working on the file

2. Employees will not leave sensitive papers out on their desks when they are away from their work stations.

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

4. Passwords will not be shared or posted near work stations.

Identity Theft Prevention Program Review and Approval

This plan has been reviewed and adopted by the Utility Board of Directors by motion during the April 14, 2014 meeting. Appropriate employees have been trained on the contents and procedures of this Identity Theft Prevention Program.

Board Chairman

Attest:

Secretary

Name of Senior Management Staff Person: N. Warren Miller

Position: Executive Director

Date: 04/14/2014

Signature: N. W~ Miller

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.

Appendix A
Other Security Procedures

The following suggestions are not part of or required by the Federal Trade Commission's "Identity Theft Red Flags Rule". The following is a list of other security procedures a utility should consider to protect consumer information and to prevent unauthorized access. Implementation of selected actions below according to the unique circumstances of utilities is a good management practice to protect personal consumer data.

1. Paper documents, files, and electronic media containing secure information will be stored in locked file cabinets. File cabinets will be stored in a locked room.
2. Only specially identified employees with a legitimate need will have keys to the room and cabinet.
3. Files containing personally identifiable information are kept in locked file cabinets except when an employee is working on the file.
4. Employees will not leave sensitive papers out on their desks when they are away from their workstations.
5. Employees store files when leaving their work areas
6. Employees log off their computers when leaving their work areas
7. Employees lock file cabinets when leaving their work areas
8. Employees lock file room doors when leaving their work areas
9. Access to offsite storage facilities is limited to employees with a legitimate business need.
10. Any sensitive information shipped using outside carriers or contractors will be encrypted
11. Any sensitive information shipped will be shipped using a shipping service that allows tracking of the delivery of this information.
12. Visitors who must enter areas where sensitive files are kept must be escorted by an employee of the utility.
13. No visitor will be given any entry codes or allowed unescorted access to the office.
14. Access to sensitive information will be controlled using "strong" passwords. Employees will choose passwords with a mix of letters, numbers, and characters. User names and passwords will be different. Passwords will be changed at least monthly.
15. Passwords will not be shared or posted near workstations.

16. Password-activated screen savers will be used to lock employee computers after a period of inactivity.

17. When installing new software, immediately change vendor-supplied default passwords to a more secure strong password.

18. Sensitive consumer data will not be stored on any computer with an Internet connection

19. Sensitive information that is sent to third parties over public networks will be encrypted

20. Sensitive information that is stored on computer network or portable storage devices used by your employees will be encrypted.

21. Email transmissions within your business will be encrypted if they contain personally identifying information.

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

23. When sensitive data is received or transmitted, secure connections will be used

24. Computer passwords will be required.

25. User names and passwords will be different.

26. Passwords will be changed at least monthly.

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

28. Password-activated screen savers will be used to lock employee computers after a period of inactivity.

29. When installing new software, vendor-supplied default passwords are changed.

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

31. Laptops are stored in a secure place.

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

33. Laptops which contain sensitive data will be encrypted

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

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

36. The computer network will have a firewall where your network connects to the Internet.

37. Any wireless network in use is secured.

38. Maintain central log files of security-related information to monitor activity on your network.

39. Monitor incoming traffic for signs of a data breach.

40. Monitor outgoing traffic for signs of a data breach.

41. Implement a breach response plan.

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

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

44. 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.

45. Implement a regular schedule of employee training.

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

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

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

49. 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.

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

51. Paper shredders will be available at the office, near the photocopier.

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