


MEMORANDUM

TO: CFX Board Members
FROM: David Taylor, Protiviti 
DATE: June 28, 2016
SUBJECT: Summary of Payment Card Industry Report on Compliance

Attached, please find the summary of the Payment Card Industry (PCI) Report on Compliance (ROC). This summary was accepted by the Audit Committee on June 23, 2016.

A summary of the ROC is provided to the Board in place of the full ROC. The full ROC is an exempt document that contains sensitive information about CFX. If any Board member would like to review the full ROC, Protiviti can arrange individual meetings, as appropriate.

Reviewed by:





*Powerful Insights.
Proven Delivery.*

Central Florida Expressway Authority

Payment Card Industry (PCI) Assessment

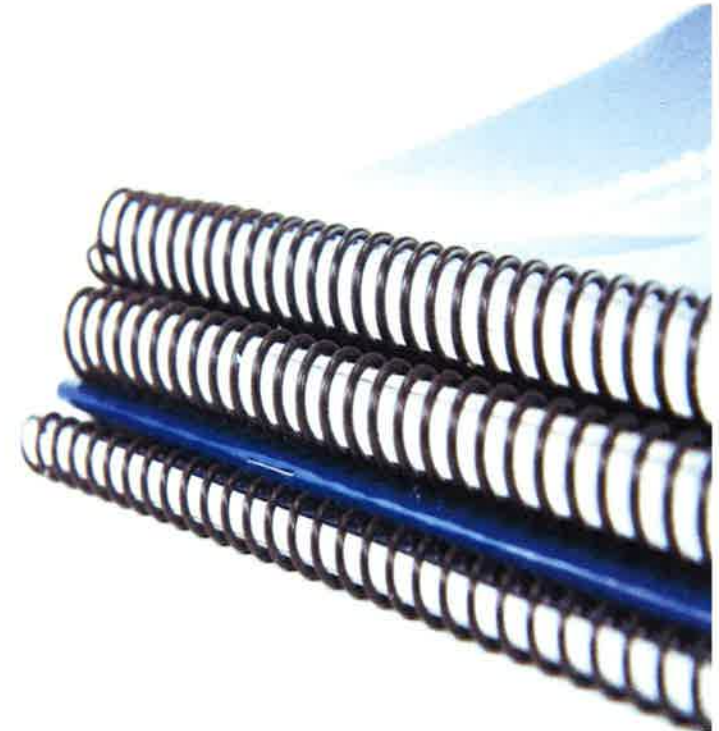
Summary Meeting

June 2016

protiviti®
Risk & Business Consulting.
Internal Audit.

Summary of the Assessment

- Protiviti team performed onsite and remote fieldwork between July 27, 2015 through April 29, 2016.
- Fieldwork was conducted through a variety of methods including documentation review, interviews, technical analysis, and physical investigation.
- In three cases, compensating controls were used to satisfy the PCI Data Security Standard.
- All CFX individuals involved were extremely helpful and well attuned to the importance of the assessment.





PCI Data Security Standard

The assessment focused on controls within the following twelve domains of the PCI Data Security Standard

Build and Maintain a Secure Network

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software or programs
6. Develop and maintain secure systems and applications

Implement Strong Access Control Measures

7. Restrict access to cardholder data by business need to know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data

Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes

Maintain an Information Security Policy

12. Maintain a policy that addresses information security for all personnel

Items of Significance

- CFX had to adjust from the PCI version 2.0 approach to segmentation to the version 3.x requirements.
- Two submission date extensions were requested by CFX and approved by BAMS to provide time for the implementation of:
 - Internal two-factor authentication
 - Application Whitelisting solution
 - Privileged account management solution
 - Virtual Observer (call quality assurance software) upgrade
- The service provider Xerox was changed to EGIS.



CFX PCI Status = Compliant

On April 29, 2016...

- ✓ **Compliant PCI Report on Compliance (ROC)** was issued by Protiviti
- ✓ **Attestation of Compliance (AOC)** was signed by Protiviti and CFX
- ✓ **Both the ROC and AOC** were submitted to Bank of America Merchant Services (BAMS)





*Powerful Insights.
Proven Delivery.®*

Confidentiality Statement and Restriction for Use

This document contains confidential material proprietary to Protiviti Inc. ("Protiviti"), a wholly-owned subsidiary of Robert Half ("RHI"). RHI is a publicly-traded company and as such, the materials, information, ideas, and concepts contained herein are non-public, should be used solely and exclusively to evaluate the capabilities of Protiviti to provide assistance to the consumer Company, and should not be used in any inappropriate manner or in violation of applicable securities laws. The contents are intended for the use of the consumer Company and may not be distributed to third parties.