Florida Department of Transportation

CHARLIE CRIST
GOVERNOR

605 Suwannee Street
Tallahassee, FL 32399-0450

STEPHANIE C. KOPELOUSOS
SECRETARY

January 21, 2010

Stephanie C. Kopelousos
Secretary
Department of Transportation
605 Suwannee Street
Tallahassee, Florida 32399-0450

RE: **Auditor General Report No. 2010-005**
Department of Financial Services and Selected Participating State Agencies
Payment Card Programs

Dear Secretary Kopelousos:

As required by Section 20.055(5)(h), Florida Statutes, attached is the six month status report for the subject audit. The report details the implementation or current status of the recommendation.

If you have any questions, please call me at 410-5823.

Sincerely,

Ron Russo
Inspector General

RR:tw

Enclosure

cc: Kathy DuBose, Staff Director
Cathy Boyett
Joint Legislative Auditing Committee
JLAC@leg.state.fl.us

Source of Audit: Auditor General
Report Number: 2010-005
Report Title: Department of Financial Services and Selected Participating State Agencies Payment Card Programs

---

Finding No. 5: Validation of Data Security Standard Compliance

The major payment card brands require merchants to validate and report PCI Data Security Standard compliance according to their merchant PCI level, which is based on payment card transaction volume over a 12-month period. In 2007, Bank of America notified DOT that the transaction volume in SunPass had reached a threshold upon which DOT was required to validate its compliance with the PCI Data Security Standard to Bank of America by September 30, 2008. As a part of these requirements, Visa established sanctions, including potential fines, for merchants who were not validated as PCI compliant by the deadline.

In response to the Bank of America notification, DOT engaged a qualified security assessor to perform a PCI Data Security Standard security assessment. Qualified security assessors are certified by the Council to validate an entity's adherence to the PCI Data Security Standard. Because DOT had engaged the qualified security assessor to validate compliance, we did not similarly evaluate applicable SunPass IT controls.

The qualified security assessor's initial assessment, dated July 30, 2008, identified 98 instances where controls required by the PCI Data Security Standard were not in place. For example, routers were not included in the firewall configuration standard, full payment card account numbers of cardholders were stored unencrypted, a formal system development life cycle based on industry best practices and secure coding was not in place, physical access to cardholder data was not appropriately restricted, and some policies and procedures required by the PCI Data Security Standard for the security of cardholder data did not exist. Under these conditions, the risk was increased that cardholder data could be breached and that sanctions could be applied by the major payment card brands.

On September 19, 2008, DOT requested an extension of the September 30, 2008, deadline to December 31, 2008. According to DOT management, Bank of America approved the extension request. SunPass was subsequently reported to have achieved PCI compliance prior to the December 31, 2008, deadline and no sanctions were assessed. Specifically, the qualified security assessor's final assessment, dated December 26, 2008, identified no areas of noncompliance. The qualified security assessor's Report on Compliance and Confirmation of Report Accuracy were reviewed by Bank of America and reported to Visa as validated for compliance with the PCI Data Security Standard.

Recommendation: Because of the volume of cardholder data retained in SunPass, DOT should closely monitor the ongoing effectiveness of SunPass security controls in complying with the PCI Data Security Standard and protecting cardholder data.

Initial Response: Florida's Turnpike Enterprise concurs and acknowledges the finding and recommendation. Due to the volume of credit card and customer information processed and managed by the SunPass program, we have and will continue to focus our efforts on protecting the confidentiality, integrity and availability of customer data.

Current Response: Florida's Turnpike Enterprise continues to protect the integrity, availability and confidentiality of credit card and customer information processed and managed by the SunPass program. To this effect the SunPass program achieved PCI compliance on December 2009 for the second time. This demonstrates our commitment to protect our customer data and maintain a good security posture.

Completed: December 31, 2009