



CITY OF ORLANDO

Office of Audit Services and Management Support

MEMORANDUM

To: Ray Elwell, Deputy Chief Financial Officer
Gene Bernal, Police Deputy Chief
Conrad C. Cross, Chief Information Officer
Robert Bowden, Leu Gardens Executive Director
Scott T. Zollars, Parking Division Manager

From: Beryl H. Davis, CPA, CGFM, Director
Audit Services and Management Support

Re: Follow-Up Review of Audit of Payment Card Personal Information Security
(Report No. 07-13)

Date: June 21, 2007

Attached is a summary of the status of our recommendations as determined from our follow-up review of the Audit of Payment Card Personal Information Security (Report No. 06-17) issued July 31, 2006. Our follow-up was made in accordance with generally accepted government auditing standards, except that we did not perform substantial tests of evidence supporting the replies from the officials responsible for resolving audit findings and recommendations.

Four of the five recommendations contained in the original report have been implemented. One recommendation is planned for implementation. The recommendation planned for implementation is expected to be implemented by September 2007 when a planned City Policy and Procedure change is finalized.

We will follow up on the status of the recommendation not fully implemented during our annual review of open recommendations in all City departments.

We wish to thank the officials of the departments affected by these recommendations for their cooperation with the follow-up request.

George McGowan, Manager, Audit Services and Management Support performed this follow-up review.

BHD/gjm

Attachment

c: Honorable Buddy Dyer, Mayor
Byron W. Brooks, Chief Administrative Officer
Joseph M. Robinson, Chief of Staff
Rebecca W. Sutton, Chief Financial Officer
Allen Johnson, Centroplex Director
Roger D. Neiswender, Transportation Director
Michael J. McCoy, Police Chief

REPLY AND IMPLEMENTATION SUMMARY
FOLLOW-UP REVIEW OF AUDIT OF PAYMENT CARD PERSONAL INFORMATION SECURITY

#	RECOMMENDATIONS	RESPONSE	CURRENT STATUS	IMPLEMENTATION DATE	AUDITEE COMMENTS
1.	The Comptroller Division should include guidance regarding the processing of payment card transactions, with information on properly securing, storing and destroying associated sensitive information, in its current revisions to City Policies and Procedures.	Concur	Planned for Implementation	No later than September 2007	We have revised our P&P to include verbiage on Payment Card Personal Information Security requirements.
2.	The Technology Management Division should periodically update the <i>Payment Card Industry Self-Assessment Questionnaire</i> , at least whenever affected applications and databases are upgraded or replaced.	Concur	Implemented	Ongoing	The Technology Management Division is ensuring that any Payment Card system that is implemented or upgraded is done so in conjunction with the guidelines put forth in the most current version of the Payment Card Industry (PCI) Data Security Standard (DSS). TM Security is responsible for ensuring that our systems adhere to the current standards that are imposed by the PCI Standards Security Council and thus, we do not actually make changes to the questionnaire; but rather we ensure that the most current version of the guidelines published by the PCI Standards Security Council is utilized.

REPLY AND IMPLEMENTATION SUMMARY
FOLLOW-UP REVIEW OF AUDIT OF PAYMENT CARD PERSONAL INFORMATION SECURITY

#	RECOMMENDATIONS	RESPONSE	CURRENT STATUS	IMPLEMENTATION DATE	AUDITEE COMMENTS
					<p>In addition, TM is coordinating with any City client and their vendor to ensure that all controls are in place. The tool utilized to facilitate this is the Payment Card Industry (PCI) Data Security Standard Self-Assessment Questionnaire that was also developed by the PCI Standards Security Council. The Technology Management team continually monitors the PCI Standards Security website to ensure that we are utilizing the most current versions of the guidelines and questionnaire.</p>
3.	<p>The Parking Division should contact the vendors responsible for the systems used to process payment card transactions and require them to complete the <i>Payment Card Industry Self-Assessment Questionnaire</i>.</p>	Concur	Implemented	August 2006	<p>Questionnaires were sent out and have been submitted to Parking.</p>
4.	<p>The Parking Division should include in future Requests for Proposals for the systems used to process payment card transactions that the vendors meet the requirements of the Payment Card Industry Data Security Standard.</p>	Concur	Implemented		<p>No Requests for Proposals have been accomplished for the systems used to process payment card transactions. Future RFPs will include the requirements.</p>

REPLY AND IMPLEMENTATION SUMMARY
FOLLOW-UP REVIEW OF AUDIT OF PAYMENT CARD PERSONAL INFORMATION SECURITY

#	RECOMMENDATIONS	RESPONSE	CURRENT STATUS	IMPLEMENTATION DATE	AUDITEE COMMENTS
5.	The managers responsible for the revenue collection process in the "Cop Shop" and Mennello Museum should ensure that these areas meet the <i>Payment Card Industry Data Security Standard</i> regarding the masking of account numbers printed on point of sale receipts.	Concur	Implemented	December 2006 for Cop Shop and March 2007 for Mennello Museum	