



AUDIT OF PAYMENT CARD

PERSONAL INFORMATION SECURITY

Release Date: July 31, 2006

Report No. 06-17

CITY OF ORLANDO

OFFICE OF AUDIT SERVICES AND MANAGEMENT SUPPORT

Beryl H Davis, CPA, CGFM
Director

George J. McGowan, CPA
Manager

TABLE OF CONTENTS

Memorandum.....	1
Background	3
Summary of Recommendations and Responses	4
Issues and Recommendations	5
Include Section on Securing Payment Card Information in Policy Revision	6
Periodically Update Payment Card Security Checklist.....	8
Ask Parking System Vendors to Complete Payment Card Security Checklist.....	8
“Mask” Payment Card Account Numbers on Point of Sale Receipts	10
Exhibit 1.....	12



CITY OF ORLANDO

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
Samuel G. Vennero, Parking Division Manager

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

Date: July 31, 2006

Subject: Audit of Payment Card Personal Information Security (Audit Report No. 06-17)

The Office of Audit Services and Management Support has performed an audit of payment card personal information security. Our objective was to determine whether procedures and controls over the protection of client personal debit/credit card information used by the City of Orlando are operating effectively. At our request, the City's Information Security Administrator in the Technology Management Division (TM) performed a review of the controls over the protection of personal information (i.e., personal payment card information) in electronic form. Audit Services and Management Support performed a review of the controls over the protection of personal information on paper documents generated during payment card transactions.

Our examination was conducted in accordance with generally accepted government auditing standards, except that we did not perform supplemental tests of the work performed by the TM. Our procedures included a review of the report prepared by TM, a review of the practices of several divisions and sections regarding their acceptance of debit or credit cards (i.e., payment cards) to pay City fees and charges and a limited examination of related documents.

Overall, we found that the City has procedures in place to protect the personal information of its fee payers. The TM memoranda noted that the City meets the necessary requirements to protect such information. This report identifies additional methods to enhance the security of the information that is gathered by the divisions that accept payment cards for City fees.

We would like to express our appreciation to the employees consulted during this audit for their courtesy and cooperation.

BHD/am

c: Honorable Buddy Dyer, Mayor
Cheryl J. Henry, Chief of Staff
Rebecca W. Sutton, Chief Financial Officer
Kevin J. Edmonds, General Administration Director
Allen Johnson, Centroplex Director
Roger Neiswender, Transportation Director
Michael J. McCoy, Policy Chief
Robert Bowman, Fire Chief
Lisa E. Early, Families, Parks and Recreation Director
Alana C. Brenner, City Clerk

BACKGROUND

The payment card industry requires merchants that store, process or transmit cardholder data to comply with its *Cardholder Information Security Program (CISP)*. One aspect of this program is that merchants must adhere to the *Payment Card Industry Data Security Standard*. The data security standard is a 12 point list of security requirements and includes a comprehensive checklist (*Payment Card Industry Self-Assessment Questionnaire*), which can be used by merchants to evaluate controls over the protection of personal payment card information.

Through discussion with key accounting personnel in each department and the Fiscal Manager for the Comptroller Division, we determined that the sections responsible for revenue collection activities in the City and that regularly accept payment cards for these activities are: Greenwood Cemetery (Executive Offices); Centroplex Box Office, Mennello Museum and Leu Gardens (Centroplex Department); Vehicles for Hire and “Cop Shop” (Orlando Police Department), the Recreation Division (Families, Parks and Recreation Department); Fire Department (for Fire permit fees and off-duty employee reimbursements) and Parking Division (Transportation Department). We also reviewed the Cashier (Finance Department), which is responsible for processing payments generated by the Permitting Division and others.

As most payment card transactions performed by the City involve electronic systems, Audit Services and Management Support consulted with the Technology Management Department (TM) to understand the controls over this sensitive information. It was determined that TM would complete the self-assessment questionnaire and provide Audit with expertise to understand whether the City has the controls in place to protect payment card information. In April 2006, TM completed the questionnaire and issued a brief report (see Exhibit 1). The TM Information Security Administrator concluded, “while the City of Orlando meets the necessary requirements to protect all information, to include payment card transactions, we endeavor to improve or elevate system security as new threats continue to challenge our integrity.”

TM noted that they did not review paper or faxed payment card transactions. Therefore, Audit Services and Management Support reviewed the controls over the paper-based documentation that may exist in the sections that accept payment cards in payment of City fees and charges. Audit Services and Management Support met with knowledgeable managers and employees in these areas to understand the practices, procedures and controls over any paper documents that may contain personal payment card information.

SUMMARY OF RECOMMENDATIONS AND RESPONSES

RECOMMENDATIONS	RESPONSES
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
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
3. 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> .	Concur
4. 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.	Concur
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

ISSUES AND RECOMMENDATIONS

- Objective** The objective of this audit was to determine procedures and controls over the protection of personal debit/credit card (i.e., payment card) information gathered by the City.
- Scope** The scope of this audit includes procedures in effect during fiscal year 2005-06.
- Methodology** The Office of Audit Services and Management Support consulted with the Technology Management Division (TM) to understand the protection of sensitive data contained in the systems used to process revenue collection transactions.
- TM agreed to review the controls in the electronic systems of the City and completed the *Payment Card Industry Self-Assessment Questionnaire* recommended for use by payment card merchants to review security over payment card personal information security.
- Audit Services and Management Support consulted with knowledgeable accounting personnel in each department and the Fiscal Manager for the Comptroller Division to determine the sections that accept payment cards for City fees and charges. Audit Services performed site visits and interviews of employees and managers most knowledgeable about the procedures and practices followed in these areas. We reviewed the controls over any written documents (receipts, faxes, forms) that contain payment card personal information.

**Include Section
on Securing
Payment Card
Information in
Policy Revision**

During this review, we learned that the Revenue Collection section of the Comptroller Division has three policies that apply to the collection of City revenues. We were informed that these policies are currently under revision. Our review of the existing policies and the current draft revisions revealed that they do not contain any guidance regarding the acceptance of payment cards.

We discussed this with the MBA Fiscal Manager, who agreed that the need to secure this information has become more important over the past few years. We found that the individuals responsible for processing payment card transactions were not aware of all of the requirements of the *Payment Card Industry Data Security Standard*. Some specific instances of non-compliance follow.

First, when discussing the procedures followed by the Recreation Centers, we learned that it was unclear whether the Centers were collecting payment card information manually to process at a later time or asking the patrons to return when the system is operational, when their cash collection system was not operational for any reason. While the Recreation Division has its own internal cash collection procedures, they currently do not address the need to secure payment card information. A comprehensive City-wide policy and procedure that addresses the proper method to secure sensitive payment card information would be helpful to define acceptable procedures when automated systems are down.

Second, while reviewing the procedures at Leu Gardens, we learned that the daily revenue collection reconciliation reports include a printed report that contains the full payment card number. In addition, we were told that after these documents are prepared, they are stored in boxes in a vacant cubicle. The *Payment Card Industry Data Security Standard* suggests that those that accept payment cards “physically secure all paper and electronic media that contain cardholder information.” The standard does not elaborate on whether

incomplete information (which shows payment card number only and not the name and expiration date) is required to be secured, but we believe that all revenue collection reports and documents should be secured in locked file cabinets to heighten their security. A policy regarding the proper storage of such sensitive information can be included in City Policies and Procedures.

Third, during our review we were told by most of the sections that process payment card transactions, that they send their daily revenue collection documents to City Archives for long-term storage when necessary due to limits on onsite storage. (Centroplex is the exception as they shred documents that contain payment card information one year after the associated event). The *Payment Card Industry Data Security Standard* recommends, “cardholder information storage should be kept to a minimum,” and that a “data retention and disposal policy should be developed.” We learned that City Records and Archives does not have a separate policy regarding the proper retention and disposal of payment card information and follows the guidance of the State of Florida in this area.

For these reasons, we believe that the City-wide Policies and Procedures administered by the Comptroller Division is the proper location for the guidance needed for the employees throughout the City that process payment card transactions. It is important to demonstrate a Citywide commitment to securing the sensitive information gathered during the transactions made by each responsible section and department responsible. Further, we suggest that the Division consider writing a separate policy for the processing of payment card transactions, as is currently done for the processing of checks. In this way, the policy can be comprehensive and include all necessary provisions.

Recommendation 1. We recommend that the Comptroller Division 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.

Response Concur. We will incorporate your recommendation in the revision of our policies.

**Periodically
Update Payment
Card Security
Checklist**

As stated, TM used the *Payment Card Industry Self-Assessment Questionnaire* to review whether the City is currently meeting the requirements of the *Payment Card Industry Data Security Standard*. This questionnaire is a comprehensive guide that identifies the best practices in the area of data security and could be used by TM to periodically review the security of the City's applications and databases.

We believe the questionnaire should be updated whenever an application or database involved in the processing of payment card information is upgraded or replaced. In this way, the items on the questionnaire are re-evaluated and TM periodically reviews the security of sensitive information.

Recommendation 2. We recommend that the Technology Management Division periodically update the *Payment Card Industry Self-Assessment Questionnaire*, at least whenever affected applications and databases are upgraded or replaced.

Response TM concurs with the recommendation.

**Ask Parking
System Vendors
to Complete
Payment Card
Security
Checklist**

We reviewed the payment card transactions of the Parking Division and learned that they use four electronic systems to process the various transactions involving payment card information. The Clancy Parking Ticket Management System is used to process both on site and online parking violations payments, the McGann Garage Access Control System is used to process monthly fees for long-term rentals of spaces in the parking garages, Worldwide Interactive Services, Inc. provides an interactive voice response system to allow patrons to make

payments by telephone and the Schlumberger system processes payments made to the master parking meters in parking lots under Interstate 4. Parking further explained that it uses a third party processing agent (ICVERIFY) to process the payment card transactions made through the McGann and Schlumberger systems.

The systems used by Parking are not included among the City electronic systems that are supported by TM. Rather, due to the vendors need to protect their systems for proprietary reasons, the systems are maintained through contracts with the vendors. Therefore, the controls over the payment card information that is processed through these systems has not been reviewed by TM and are the responsibility of the vendors. We believe that the City may be exposed if there are any problems or control weaknesses in the security of this payment card information. Therefore, it is important for the City to get an assurance from the vendors that they are aware of the Payment Card Industry Data Security Standards.

First, we believe that the Parking Division should contact the vendors responsible for the systems used to process payment card transactions and ask them to complete the Payment Card Industry Self-Assessment Questionnaire. Next, when the contracts for these services expire and new Requests for Proposals for these services are prepared, the Division should include a requirement for the vendors to demonstrate that they have met the requirements of the Payment Card Industry Data Security Standard and will continue to meet these requirements during the term of their contract with the City.

Recommendation 3. We recommend that the Parking Division contact the vendors responsible for the systems used to process payment card transactions and require them to complete the *Payment Card Industry Self-Assessment Questionnaire* to document that they have the required controls over sensitive information.

Recommendation 4. We recommend that the Parking Division 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.

Response

We concur with the recommendations and will get a copy of the questionnaire out to Clancy, Worldwide and ICVERIFY (processing agent for the McGann and Schlumberger systems) for completion. We will ensure it is in future RFPs.

**“Mask” Payment
Card Account
Numbers on
Point of Sale
Receipts**

We reviewed the receipts issued by sections that accept payment cards for City fees and charges, and learned that two sections (Cop Shop and Mennello Museum) currently issue receipts that list the entire payment card number and expiration date.

We also noted that the receipts issued by the areas using the Cashiering for Windows system (Cashier, Vehicles for Hire, Greenwood Cemetery) mask the last four digits of the payment card number. The Cashiering for Windows system is an integrated point of sale cashiering system managed by the Accounting and Control Division and utilized throughout the City to account for revenue transactions.

The other areas reviewed (Centroplex Box Office, Leu Gardens and Recreation) mask all but the last four digits of the number.

The payment card number is sensitive information and showing the entire number and expiration date could increase the risk that someone other than the cardholder will utilize the payment card. Apparently, when the equipment used to swipe payment card information and print a manual receipt to the customer were acquired or updated, the standard to “mask” (i.e., hide) a portion of the payment card account number was not known. The *Payment Card Industry Data Security Standard* recommends that the first six and last four digits be the maximum number of digits to be displayed.

The security of City fee and charge payer’s payment card number should be increased by meeting the recommendation of

the *Payment Card Industry Data Security Standard* with regards to “masking” the payment card account number when it is displayed on a paper receipt or otherwise retained as documentation for cash collections.

Recommendation 5. We recommend that the managers responsible for the revenue collection process in the “Cop Shop” and Mennello Museum ensure that these areas meet the *Payment Card Industry Data Security Standard* regarding the masking of account numbers printed on point of sale receipts.

Response OPD concurs with the recommendation and has begun efforts to implement it.

Centroplex management concurs and has asked staff to proceed with acquiring a new system. We anticipate the software to be functional prior to the end of the fiscal year.

EXHIBIT 1

To: John Matelski, Deputy Chief Information Officer / CSO
George McGowan

From: Vernon Greene, Information Security Administrator / CISO

Date: 04 April 2006

Subject: Payment Card Audit

Narrative

Review of payment card transactions and standards used if governed by the City of Orlando. Please review the attached checklist for compliance.

Actions taken by the ISO

- Current Security Status and standards reviewed
 - Review of current security procedures and policies for secure transactions meet all necessary requirements.
 - Firewalls, routers and wireless access security is in place
 - Antivirus, Intrusion detection and spyware scanners are functioning to security specifications
 - System authentication meets standards by deploying LDAP, IPSEC, VPN and C2 to name a few
 - Policies are modified to meet current technology challenges and reviewed frequently
- Review of use and government
 - Permitting, Centroplex, Family Parks and Receptions and Parking Bureau all perform payment card transactions which are not retained locally, but instead sent to the third party companies such as Verisign or Ticketron.
 - As noted in the checklist, any information seen locally will not reveal in full the payment card numbers or security codes.
 - Paper handling or faxed payment card transactions were not reviewed in this process
- Security of confidential information
 - Protection of confidential information is handled by both logical and physical measures. First, by enforcing security best practices when the users sign on to their computers, encrypting the data collected and passing the data to its final destination. Second, any information housed on servers locally are monitored and protected from foreign attacks such as viruses or intrusions.
 - CONCERT (City of Orlando Computing Emergency Response Team) is formed to mitigate threats that do make it through.

Security Remarks

While the City of Orlando meets the necessary requirements to protect all information, to include payment card transactions, we endeavor to improve or elevate system security as new threats continue to challenge our integrity.