Office of the City Auditor

CONSENT CALENDAR
May 31, 2011

To: Honorable Mayor and Members of the City Council

From: Ann-Marie Hogan, City Auditor

Subject: Audit of Citywide Payment-Card Acceptance: Is Cardholder Information Safe?

RECOMMENDATION

Request the City Manager report back by January 31, 2012, and every six months thereafter regarding the implementation status of each recommendation in the attached audit report until all recommendations have been reported implemented.

SUMMARY

1) Has the City addressed the PCI DSS?
   Approximately 36 City locations or operations accept payment cards for fees, fines, and other financial obligations to the City. The City is subject to the Payment Card Industry Data Security Standard (PCI DSS), which includes data security requirements designed to protect customer account information and prevent fraud. Wells Fargo provided a PCI DSS consultant to assist with required annual compliance questionnaires and network security scans. Wells Fargo found that all City locations are now compliant.

2) Do City operations that accept payment cards have controls in place to protect cardholder information?
   Generally, the payment-card operations we observed have controls in place to protect cardholder information. However, the 311 Call Center, the Permit Service Center, the Office of Vital Statistics, and the Berkeley Marina need to improve physical security of cardholder information. Staff in these units could capture and misuse this information. We have no evidence that such misuse has occurred.

3) How much does it cost to accept payment cards in payment of financial obligations to the City?
   Council members asked the City Auditor why the City does not accept more online transactions. This report discusses some of the risks and costs of doing so. In FY 2010, the City paid almost $423,000 in bank and payment-card industry fees, or about 2.4 percent of just under $17.5 million in gross payment-card revenue. The cost for parking meters ranges from 15 percent to almost 20 percent. Also, acceptance of payment cards at parking meters likely reduces revenue from parking

fines. From FY 2007 through FY 2010, revenue from parking-meter fees increased almost $1 million, while revenue from parking fines decreased by almost $2.6 million.

Though responsible for coordinating citywide payment-card activities, Finance has not issued guidance to City Departments on requirements and responsibilities when accepting payment cards.

Finance had discontinued providing cash handling training and conducting surprise cash counts. Cash handling training includes training in processing payment-card transactions. Surprise cash counts normally cover daily cash balancing, including payment card transactions. Staffing reductions due to budget cuts might be eroding important fiscal controls.

FISCAL IMPACTS OF RECOMMENDATION

Implementing our audit recommendations to provide guidance and training and to consider options for protecting cardholder information can reduce the City's risk that City staff could capture and misuse that information. The City received almost $17 million in net payment card revenue in fiscal year 2010. The City could have been subject to monetary penalties if noncompliant with the PCI DSS.

RATIONALE FOR RECOMMENDATION

The lack of written guidance makes it more difficult to monitor payment-card activities and increases the risk that these activities might not be optimized for the City's needs or responsibilities.

Our 2002 Citywide Cash Receipts / Cash Handling survey identified 94 locations that received or handled cash or cash equivalents totaling just under $70 million annually. With that level of cash activity, it is critical that personnel who handle cash receive cash handling training and that they know they might be subject to a surprise cash count at any time.

CONTACT PERSON

Ann-Marie Hogan, City Auditor, 981-6750

Attachment
1. Audit of Citywide Payment Card Acceptance: Is Cardholder Information Safe?

Attachment 1

City of Berkeley

Payment-Card Acceptance Audit:
Is Cardholder Information Safe?

Prepared by:

Ann-Marie Hogan, City Auditor, CIA, CGAP
Harriet Richardson, Audit Manager, CPA, CIA, CGAP
Jack Gilley, Auditor II, CFE

Presented to Council May 31, 2011

2180 Milvia Street, Berkeley, CA 94704 ♦ Tel.: (510) 981-6750 ♦ Fax: (510) 981-6760
Email: auditor@cityofberkeley.info ♦ Web: www.cityofberkeley.info/auditor

Audit of Citywide Payment-Card Acceptance:
Is Cardholder Information Safe?

Table of Contents

I. Executive Summary

Our audit objectives were to determine:

1) **If the City has addressed the Payment Card Industry Data Security Standard (PCI DSS).**
2) **If City operations that accept payment cards have controls in place to protect cardholder information.**
3) **The cost of accepting payment cards in payment of financial obligations to the City.**

Has the City addressed the PCI DSS?

The City is required to comply with the PCI DSS, and the Departments of Finance and Information Technology (IT) worked together to address compliance. Wells Fargo provided a PCI DSS consultant to assist with required annual compliance questionnaires and conduct a required quarterly network security scan at sites the consultant identified. Wells Fargo found that all City locations are now compliant.

Do City operations that accept payment cards have controls in place to protect cardholder information?

Generally, the payment-card operations we observed have controls to protect cardholder information. However, the 311 Call Center, the Permit Service Center, the Office of Vital Statistics, and the Berkeley Marina need to improve physical security of cardholder information. There is a risk that staff in these units could capture and misuse this information. We have no evidence that such misuse has occurred (Finding 2).

The City incurs high contract costs for processing parking meter payments.

How much does it cost to accept payment cards in payment of financial obligations to the City?

In fiscal year 2010, the City paid almost $423,000 in bank and payment-card industry fees, or about 2.4 percent of just under $17.5 million in gross payment-card revenue. Bank and industry fees for parking meter charges were substantially higher than 2.4 percent. The cost for certain parking meters is almost 20 percent. (See “background” below.)

Lack of Formal Policies and Procedures

Though responsible for coordinating citywide payment-card activities, Finance has not issued guidance to City departments on requirements and responsibilities when accepting payment cards in payment of financial obligations to the City (Finding 1).

II. Background

36 City locations accept payment cards.

The City has approximately 36 locations or operations that accept payment cards, including contractor-operated websites, for payment of fees, fines, and other obligations to the City. Examples include all City libraries and parking garages, the Finance Department's Customer Service Center, the 311 Call Center, the Planning Department's Permit Service Center, and the Public Works Department's Transfer Station. The City has also made arrangements to enable the public to use payment cards to make online payment of certain obligations.

Council members asked the City Auditor why the City does not accept more online transactions. This report discusses some of the risks and costs of doing so.

The City selected Wells Fargo Bank as its primary payment-card service provider. Payment-card transactions are batched and transmitted to Wells Fargo daily. Each day, Wells Fargo automatically credits a City depository account for the gross receipts from transactions submitted the prior day and charges the same account for fees and service charges related to those transactions.

The City collected almost $17 million in net revenue[1] on just over 1.4 million payment-card transactions in fiscal year 2010.[2] The City accepts VISA and MasterCard for credit transactions. At the completion of our field work, only two City locations were equipped with PIN pads that enable acceptance of any debit card.

The Call Center does not normally accept payment of parking permits, traffic fines (paid to the adjudicating court), building permits (requires documentation), or business license fees and taxes. On rare occasions, the Call Center will process a business license tax payment at the request of the Finance Customer Service Center or Revenue Collection Division.

[1] After subtraction of bank and payment-card industry fees and charges.

[2] These numbers, which are taken from schedules we received from Finance, do not include payment-card payments of registration fees for Parks, Recreation, and Waterfront Department programs through a contract with the Active Network. The Finance schedules are based on Wells Fargo Reports. Because Active Network payment-card receipts are not processed through Wells Fargo, they are not included in the schedules.

The City plans to acquire new software for business license processing. Finance is looking into accepting online payment of business license taxes and fees once the new software is in place.

Data Security Standard

The Payment Card Industry Data Security Standard (PCI DSS) is a comprehensive set of requirements established by the PCI Security Standards Council. It includes 12 core data security requirements designed to protect customer account information and prevent fraud, and numerous subrequirements. All entities, regardless of size, that accept payment cards (debit or credit), are required to comply with the PCI DSS.

All entities that accept payment cards – including the City – must comply with the PCI DSS.

The auditors became aware of risks associated with noncompliance with the PCI DSS in February 2010 by reviewing an audit report by the Phoenix City Auditor. As a result, this audit was scheduled as part of the fiscal year 2011 Audit Plan, issued on June 29, 2010.

Compliance Project

In July 2010, shortly after the audit began, Wells Fargo notified the City that the City is required to complete PCI DSS compliance self-assessment questionnaires and undergo network security scans. According to Finance, Wells Fargo had not previously notified the City of the requirement.

Wells Fargo provided a PCI DSS consultant to assist with required annual compliance questionnaires and conduct a required quarterly network security scan at sites the consultant identified. Wells Fargo offered to pay the consultant’s fee if the City was found to be compliant.

Finance and IT worked together, and with the consultant, to facilitate completion of the questionnaires and security scans.[3]

Employee Background Checks

Administrative Regulation 3.21 requires employees responsible for cash handling and asset management to undergo a background investigation. This requirement has been applied to employees hired for, or transferred to, positions that involve processing payment-card receipts. Employees who held such positions when the Administrative Regulation became effective in May 2006 were deemed exempt from the requirement.

Existing employees were exempted from background checks.

[3] The Library did not become PCI DSS complaint until February 2011 and was required to complete another self-assessment questionnaire by April 30, 2011, to remain compliant.

Cost of Accepting Payment Cards Varies

Bank and Payment-Card Industry Fees

Wells Fargo collects fees and service charges assessed by itself, the VISA and MasterCard networks, and the cardholders' issuing banks. For the year ended June 30, 2010, the City paid just under $423,000, or 2.4 percent, in fees and service charges on gross payment-card revenue of almost $17.5 million.

City of Berkeley
Summary of Payment-Card Revenue
Fiscal Year Ended June 30, 2010

Gross Revenue	Fees & Service Charges	Adjustments & Chargebacks[4]	Net Revenue	Number of Transactions
$17,472,250	$422,989	$57,819	$16,991,442	1,407,006

Fees and service charges on small transactions, such as parking meter charges, are assessed at a higher percentage. The City paid more than 5.7 percent in bank and payment-card industry charges on payment-card revenue from Cale Parking Systems meters,[5] and 7.3 percent on payment-card revenue from IPS Group meters.[6]

Contractor Processing Fees

Cale and IPS also charge processing fees. The City pays Cale $9,765 per month to process payment-card transactions.[7] IPS charges 12 cents per payment-card transaction.

With fixed monthly charges, the cost per transaction varies with the number of transactions. In fiscal year 2010, Cale meter transactions averaged 100,635 per month. With this volume, if the average charge per transaction is $1.00, the City only earns 85 cents for every dollar charged:

[4] A chargeback is a reversal of a charge (credit) that an issuing bank makes to the account of a cardholder who successfully disputes a charge on his/her billing.

[5] The City acquired Park EZ multi-space pay and display meters that accept payment cards from Cale Parking Systems USA, Inc.

[6] The City leases single-space meters that accept payment cards from IPS Group, Inc., under a pilot program. Processing charges cover use of the meters.

[7] The City has 217 Cale meters @ $45 per meter per month ($25 for wireless communication plus $20 for processing).

It costs more to accept payment cards for parking-meter fees.

Gross parking-meter fee		$1.00
Less:		
Bank/payment-card industry fees and service charges:	(.057)	
Cale data transmission and online processing charges: ($9,765/100,635)	(.097)	(.15)
Net revenue		$.85

The City purchased 217 Cale meters at a price of $7,812 each, for a total purchase cost of $1,695,204. We did not attempt to determine how much the payment-card feature added to the cost of the meters.

If the average transaction amount at IPS parking meters is also $1.00, the City earns only 80.7 cents per dollar charged:

Costs for some operations are almost 20%.

Gross parking-meter fee		$1.00
Less:		
Bank/payment-card industry fees and service charges:	(.073)	
IPS transaction fee:	(.120)	(.193)
Net revenue		$.807

Meter fees up $1 million – Fines down $2.4 million

Another potential impact of accepting payment cards is that the City will likely experience a decline in revenue from parking fines. If the meters accept payment cards, it is logical that drivers are more likely to pay in full because they do not have to rely on having cash. City Budget documents note a decline in ticket writing, from just under $11.6 million in FY 2007 to $9.02 million in FY 2010. This almost $2.6 million decline in parking-fine revenue occurred during a period in which revenue from parking-meter fees increased by almost $1 million.[8]

[8] Source: FY 2010 & FY 2011 Adopted Biennial Budget and FY 2011 Adopted Mid-Biennial Budget Update. We do not know to what extent this decline is due to payment-card acceptance or to other factors, such as the economic decline. It should be noted that parking fines are a substantially greater source of revenue than parking-meter fees. In fiscal year 2010, the City received less than $5.4 million in parking meter fees.

Accepting payment cards, on the other hand, helps reduce the City's costs for depositing coins. According to Finance, the City pays from $10,000 to $12,000 per month for an armored courier service to count and deliver the coins to Wells Fargo for deposit. The bank also assesses a service charge for accepting coins on deposit. The courier and bank charges are based on volume.

III. FINDINGS AND RECOMMENDATIONS

Finding 1: Provide Guidance to Departments that Process Payment-Card Receipts

The Finance Department had not issued guidance that covers a City department's responsibilities and obligations from accepting payments via payment cards. Finance is responsible for coordinating City financial operations, including coordinating citywide payment-card operations. This responsibility covers all interaction with Wells Fargo and ensuring that payment-card revenues are accurately recorded and reported.

The lack of adequate written guidance makes it more difficult to monitor payment-card activities. It also increases the risk that a department's payment-card activities might not be optimized for the City's needs or responsibilities. Examples of problems that might have been avoided if written policies and procedures had been in place include:

Four payment-card service contracts did not require PCI DSS compliance.

- The City awarded four service contracts that involve processing of payment-card receipts. They did not include requirements for the contractors to comply with the PCI DSS.[9]

  Subsequent to the start of our audit, Finance and the Department of Information Technology (IT) worked together to obtain assurance that the contractors are compliant. IT assured the auditors that, going forward, all new contracts involving payment-card payments will have provisions for PCI DSS compliance.

[9] The contracts did have data security requirements, but did not specifically address the PCI DSS. Due to the many PCI DSS subrequirements, a card processor could have extensive security features and still not fully comply with the PCI DSS.

- Payment-card payments received by the Active Network[10] are not processed through Wells Fargo. As a result, the City's ability to use the revenue is delayed. Wells Fargo credits a City deposit account for payment-card revenue, but the Active Network issues checks, which are received and deposited by Parks. The City loses interest for the float period between the date that Active Network writes a check and the date the deposit ultimately clears.

- The Systems Accountant was concerned that Parks' accounting for Active Network payment-card revenue is coded as check receipts. She said it would be much easier for Finance to determine the City's total payment-card revenue if Parks' entries were coded to distinguish revenue from payment-card transactions, as opposed to revenue from other payment types.

City Manager's Response to Finding:

Agree.

Recommendation for Finance and City Manager's Response:

1.1 Issue an administrative regulation to define the responsibilities, obligations, and requirements for City departments that accept payment cards in payment of financial obligations to the City.

Agree. A new administrative regulation will be issued by January 31, 2012, to describe obligations and requirements for City departments that accept payment cards. The AR will address visibility and security of cardholder information.

[10] The City contracted with the Active Network for online recreation program registration, including accepting payment cards for registration fees. The City discontinued online registration but still uses Active to process payment-card transactions and provide a variety of reports.

Finding 2: Improve Security Over Cardholder Information at the 311 Call Center, Permit Service Center, Office of Vital Statistics, and Berkeley Marina

It would be possible for staff who process payment-card receipts at the 311 Call Center, the Permit Service Center, the Office of Vital Statistics, and the Berkeley Marina to capture cardholder information without being observed by the supervisor, or by another employee. Once captured, cardholder information could be used for inappropriate purposes. The risk of misuse of cardholder information is illustrated by recent events at an airline ticket counter in San Jose.[11]

311 Call Center

It would be possible for staff to capture and misuse cardholder information.

Citizens can call 311 and use their payment cards to pay most types of financial obligations to the City. Since Call Center staff work in separate cubicles, one would not likely be observed if writing down cardholder information, such as the customer's name, address, and payment-card number.

The Call Center Supervisor told us that Call Center staff are not permitted to write down a customer's payment-card number. The current version of Finance's Cash Handling Training Manual does not prohibit recording cardholder information when processing payment-card transactions, though a prior version did. The Call Center uses this manual as its only written procedures.

Permit Service Center

Property owners can apply for a building permit at the Planning Department's Permit Service Center. If an applicant does not wish to apply in person,[12] he/she may submit a Credit Card Authorization Form to pay the application fee by payment card. The application and Credit Card Authorization Form are kept in an unsecured location until a Permit Specialist is available to process the application.[13] It would be possible for an employee to capture cardholder information from an authorization form without being observed.

Vital Statistics

The Department of Health Services' Office of Vital Statistics processes applications for birth and death certificates, including applications received by mail. Mail-in applicants may pay for the requested

[11] The *San Francisco Chronicle* reported on February 17, 2011, that an airline ticket agent at the Mineta San Jose International Airport stole customer credit card data and used it to make over $480,000 in fraudulent purchases.

[12] i.e., the application is either faxed to or dropped off at the Permit Service Center.

[13] If not processed by the end of the work day, the documents are moved into a safe until the next work day.

certificate by check, money order, or credit card[14] (by entering their credit-card information on the application form). The employee who processes these applications works in a partitioned cubicle that cannot be viewed from other work stations. With this arrangement, cardholder information could easily be captured with little risk of being observed.

Vital Statistics, which is co-located with the Finance Customer Service Center, has only three employees, including the unit's supervisor. There are likely to be times when the employee processing credit-card payments will be the only Vital Statistics employee present, increasing the likelihood that the capture of cardholder information would not be observed.

Vital Statistics stores applications for one year.[15] Though staff made an effort to redact credit-card information before storing, we found that it was still readable.

Berkeley Marina

The Berkeley Marina accepts payment cards for security deposits on temporary (visitor) berth rentals. Instead of charging the card at the time of rental, the renter is asked to fill out a form that captures the cardholder's name, address, credit card number, expiration date, and card verification value code (V-code). This form is kept in an unsecured location. Eight Marina staff have access to the forms.

The V-code is the three digit nonembossed number on the signature panel on the back of a VISA or MasterCard. With the V-code, the form contains all information needed to use the payment card for online purchasing.

City Manager's Response to Finding:

Generally Agree.

[14] Applicants also have the option of applying in person or by internet through VitalChek.com. When applying in person, the applicant can pay by cash, personal check, postal or bank money order, or debit card. A $2.50 service charge applies to debit card transactions. VitalChek charges a $6.00 service charge for internet purchases.

[15] According to Vital Statistics staff, the forms are stored in a locked file cabinet in a storage room, which is also locked after hours. Only Vital Statistics staff have access to the storage room.

Recommendations for Information Technology and City Manager's Response:

2.1 Replace the existing cubicle partitions in the 311 Call Center with transparent Plexiglas.

Agree. The Call Center will contract with a vendor to redesign the work space to include either transparent partitions or lowering the partitions so all Customer Service Agents can see each other's work space. This work should be completed by December 31, 2011.

2.2 Consider establishing camera surveillance in the 311 Call Center.

IT will consider the recommendation, and make a decision by January 31, 2012. Implementation will be dependent on the availability of funding. IT indicated that a complete business analysis should be conducted to determine the feasibility.

Recommendations for Planning and City Manager's Response:

2.3 Consider placing faxed and dropped-off permit applications and Credit Card Authorization Forms in a dual custody lock box or file cabinet until processed, with no employee holding the key or combination to both locks.

2.4 Consider establishing camera surveillance at the Permit Service Center.

The Director of Planning expressed reservations about the finding and Recommendations 2.3 and 2.4. Planning will consider the recommendations and report back to Council by January 31, 2012.

Recommendations for Finance and City Manager's Response:

2.5 Revise the Cash Handling Training Manual to specifically prohibit writing down a payment-card holder's name, address, or payment-card number. Include this prohibition in the administrative regulation to be developed under Recommendation Number 1.1 above.

Agree. The training manual will be revised by January 31, 2012.

Recommendation for Health Services and City Manager's Response:

2.6 Consider options for reducing the risk that Vital Statistics staff could capture cardholder information for inappropriate use. Possibilities include:

- Eliminate partitions.
- Require involvement of two employees to process credit-card payments.
- Establish camera surveillance.
- Start accepting credit cards at the Customer Service counter and discontinue accepting payment by credit cards with mail-in applications. The Vital Statistics' webpage could advise customers that if they need to use credit cards, they must do so in person at the Customer Service Center or via VitalChek.com.

Agree. Effective April 11, 2011, Vital Statistics discontinued accepting payments by credit card with mail-in applications. Vital Statistics' webpage advises customers that if they need to use credit cards, they must do so via VitalChek.com. This action does not adversely impact Vital Statistics customers because direct pay card purchases represent only 0.8 percent of the total requests the City receives for birth and death certificates. This represents annual revenue of approximately $3,000 or 1 percent of Vital statistics total annual revenue of $257,000. Recommendation 2.6 is fully implemented.

Recommendation for Parks, Recreation and Waterfront and City Manager's Response:

2.7 Take action to reduce the risk that Marina staff could capture cardholder information for inappropriate use. Possibilities include:

- Discontinue accepting payment cards for berth rental deposits.

- Charge the payment card at the time of rental, and execute a credit (refund) transaction when the key is returned.

Agree. Finance and the Marina are working on a solution and will most likely adopt the second option above. A decision on the option selected will be made by May 31, 2011.

Finding 3: Provide Citywide Cash Handling Training (Repeat Finding – May 16, 2006)

In the past, Finance provided training to City staff in processing payment-card receipts as part of cash handling training. However, Finance is not presently offering scheduled citywide cash handling training. Training is an important internal control to ensure that employees understand their requirements and responsibilities, such as the responsibility to protect cardholder information.

In a May 26, 2008, report to Council,[16] the City Manager stated that Finance is scheduled to offer cash handling classes quarterly. A Finance representative told us that in the past year the training was only provided to two City units, on request (Library and Animal Shelter). There was no citywide training. The employee who was responsible for cash handling training retired and the task has not been reassigned.

The Finance representative was unable to provide the dates of the Library and Animal Shelter training. This indicates that Finance did not maintain training records to enable verification of training.

City Manager's Response to the Finding:

Agree.

Recommendations to Finance and City Manager's Response:

3.1 Establish a target for the number of cash handling classes to be held each fiscal year. If the target is not achieved due to staffing issues, report this condition in writing to the City Manager, as recommended in our May 16, 2006, follow-up report.

Agree. Finance will establish a target date for the number of cash handling classes held each fiscal year by January 1, 2012, and report nonachievement of the target to the City Manager. Finance expects to find resources for the training from a departmental reorganization currently underway.

3.2 Maintain a record of each cash handling class, including date, location, and name and department of each attendee. The citywide training software can be used for this purpose.

[16] The report covered the status of Recommendation 5.1 in our Follow-Up Cash Receipts / Cash Handling Audit, May 16, 2006.

Agree. Finance will maintain a detailed record of each training session.

Finding 4: Resume Conducting Surprise Cash Counts

Budget cuts might be eroding important fiscal controls.

A surprise cash count provides an opportunity to review a City operation's controls over payment-card transactions. Payment-card transactions are normally included in daily transaction balancing, and transaction balancing should be reviewed in a surprise cash count. However, Finance has discontinued conducting surprise cash counts.

Surprise cash counts provide a deterrent against theft and fraud. In its 2010 Report to the Nations, the Association of Certified Fraud Examiners states that surprise audits are an important tool in the fight against fraud, and that organizations that conduct surprise audits have lower fraud losses. It also states that the greatest benefit of surprise audits is in preventing frauds by creating a perception of detection.

Surprise cash counts are a deterrent against theft and fraud.

In 2004, the Director of Finance agreed to perform approximately ten cash reviews (which would include surprise cash counts) per year in various City Departments, other than Finance. Finance staff told us that surprise cash counts have not been conducted in approximately two years due to staffing cuts. As a result, the City does not have assurance that appropriate controls are maintained over cash handling and payment-card operations, and that cash funds can be fully accounted for. Thus, there is an increased risk that fraudulent cash and payment-card transactions will occur and not be detected.

City Manager's Response to the Finding:

Agree.

Recommendations to Finance and City Manager's Response:

4.1 Establish a target for the number of surprise cash counts to be conducted each fiscal year. If the target is not achieved due to staffing issues, report this condition in writing to the City Manager.

Agree. Starting July 1, 2011, Finance will establish a target for the number of surprise cash counts to be conducted each fiscal year, and report nonachievement of the target to the City Manager in writing. Surprise cash counts will be performed in conjunction with internal control reviews, with a focus on using resources to identify and cover those locations that pose the greatest internal control risk to the City.

4.2 Maintain a record of all surprise cash counts, including date, location, and findings, such as poor controls, or cash shortages.

Agree. Starting July 1, 2011, Finance will maintain a record of surprise cash counts conducted each fiscal year.

4.3 Provide a copy of the cash count report to the department director. Also provide a copy to the City Manager.

Agree. Finance will provide a copy of the report to the affected department director and the City Manager.

IV. FISCAL IMPACT

The City received almost $17 million in net revenue from payment-card transactions in fiscal year 2010. The City was rated as PCI DSS compliant at the completion of our field work.[17] The City could have been subject to monetary penalties if noncompliant.

Misuse of cardholder information might subject the City to liability.

The City might be liable should a City or contractor employee capture cardholder information and use it to defraud the cardholder. Aside from potential litigation settlement costs, legal fees, and embarrassment to City officials, customers might reconsider using their cards to pay obligations to the City.

The Bay Cities Joint Powers Insurance Authority's (BCJPIA) insurance policy covers the City for loss due to employee theft and fraud, through the City's membership in the Authority. The policy excludes coverage of loss due to unauthorized use of third party information, including payment-card information. However, a representative of the insurance agency assured a City official that:

> …where these THIRD PARTY credit card "securities" are lawfully in the possession of the City and its "Employees" fraudulently use the information that this would be covered under the BCJPIA Crime policy….You can confirm to the auditors that this risk is properly protected.

We believe that the City's interest, and those of the other Authority members, would be best served if the policy covers such loss in writing.

[17] The Library's compliance certificate was scheduled to expire on April 30, 2011.

Our Citywide Cash Receipts / Cash Handling Survey (report date February 19, 2002) identified 94 locations in 18 departments (excluding Finance) that received and/or handled cash or cash equivalents. At that time, the cash or cash equivalents handled by these locations totaled just under $70 million annually. With so many locations handling so much cash each year, it is critical that the personnel staffing these locations receive cash handling training and that they know they might be subject to a surprise cash count at any time. Theft of just 1 percent of the cash handled at these locations would cost the City almost $700,000 annually (based on the 2002 data).[18]

Implementing our recommendations to provide guidance on payment-card processing, and to improve physical security over payment-card data, will reduce the risk of misuse of cardholder information. It will also help improve Finance's ability to monitor citywide payment-card activity. Implementing our recommendations to provide cash handling training and conduct surprise cash counts will reduce the risk of theft and fraud by strengthening general prevention and detection controls over payment-card and cash handling activities.

[18] In its 2010 Report to the Nation, the Association of Certified Fraud Examiners (ACFE) estimated that the typical organization loses 5 percent of its annual revenue due to fraud. We use a more conservative 1 percent in our estimate. More than 16 percent of the frauds reported in the ACFE study occurred at government agencies.

APPENDIX A

SCOPE AND METHODOLOGY

Our audit was limited to: 1) FY 2010 payment-card transactions, 2) current procedures at selected City operations for processing payment-card receipts, 3) City awarded contracts that provide for processing payment-card payments, and 4) efforts to address the City's PCI DSS compliance requirements. We accomplished our audit objectives by:

- Researching PCI DSS requirements.
- Interviewing Finance staff responsible for coordinating citywide payment-card activities.
- Interviewing supervisors at selected City operations that process payment-card receipts.
- Observing procedures related to payment-card transactions at selected City operations.
- Inspecting documents related to payment-card operations or transactions.
- Surveying department heads to identify contracts for payment-card processing services.
- Reviewing City contracts that cover processing payment-card transactions.

We relied on certain data provided by the Finance Department without performing audit procedures to validate the accuracy of the data or evaluating controls designed to ensure accuracy of the data. This data pertains to the volume of payment-card transactions and the amount of payment-card receipts and fees paid. Reliance on this data did not affect our findings and conclusions.

We conducted field work from July 2, 2010, through March 11, 2011, and limited it to those areas specified above. We conducted this audit in accordance with *Generally Accepted Government Auditing Standards (GAGAS).* Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our objectives.