A Performance Audit of the

Salt Lake County Treasurer's Office

A Confidential Report to the Salt Lake County Treasurer

December 2009

Jeff Hatch

Salt Lake County Auditor

A Performance Audit of the

Salt Lake County Treasurer's Office

December 2009

JEFF HATCH
Salt Lake County Auditor

JAMES B. WIGHTMAN, CPA, CISA, MBA, MAcc
Director, Internal Audit

Audit performed by:

Cherylann J. Johnson, MBA, CIA
James Fire, MBA/Acc
Scott Tingley, MSA

Table of Contents

I. Executive Summary

Background

The Salt Lake County Treasurer's Office provides statutorily mandated tax administration services to the citizens, tax entities, and government agencies of Salt Lake County. These services include the following:

- Billing, collecting, and distributing real property taxes
- Administering tax-relief programs
- Managing and investing tax proceeds and other County entrusted public monies and funds

The Treasurer's Office had 29 full-time equivalent (FTE) employees and expenditures of $3,045,901 in 2008, and 27 FTE employees and expenditures of $3,194,744 in 2009. According to Salt Lake County's Budget Document, property taxes for 2008 provided 23% ($185.5 million) and for 2009 provided 22% ($188.2 million) of the County's major revenue sources.

A number of information systems are used for recording tax revenues, such as electronic imaging and storage, online banking, and cashiering. All systems and processes eventually converge into the County's mainframe-based tax and financial systems. County Information Services (County IS) is relied on exclusively for the management, storage, and reporting of County property tax and related data.

The current mainframe tax system has been in service for more than 30 years. A Request for Proposals (RFP) for a new Tax Administration System was issued on March 16, 2009. After several RFPs were received and evaluated, the final contract was signed on December 30, 2009. The timeframe for implementation of the new system is projected to be 18 to 24 months from vendor approval.

The implementation will provide many changes to the processes used to generate journal entries in the Treasurer's Office. The most notable change will be the elimination of mainframe data exports into spreadsheets. We reviewed a multitude of spreadsheets used for the creation of journal entries for accuracy. We observed that substantial time and effort was necessary by Treasurer's personnel to ensure accuracy. The new system should provide much improved efficiency in these processes.

The Treasurer also has other non-statutory responsibilities. They include providing the Sheriff's bail and prisoner depository, collecting payments to settle dishonored checks, and facilitating County agencies to accept payment-card payments for goods and services.

Findings and Recommendations

Cashiering system totals were not compared to cash/check exchange transaction totals at the time each change fund replenishment request was prepared. (§1.1 of Report). Change order request amounts could be determined from the iNovah cashiering system reports eliminating the need to tally Cash/Check Exchange Forms (pink forms), which would:

- Reduce the risk that a fraudulent pink form could be created or an existing one altered and not be detected.
- Show discrepancies between the change fund balance and the cashiering system transaction totals that would be more easily reconcilable as replenishments are requested.

Using transaction summary reports generated by the cashiering system could add an additional level of internal control over the change fund replenishment process.

RECOMMENDATION:

The cash/check exchange transaction totals obtained from the iNovah cashiering system could be used to determine the amounts included in the change fund replenishment requests.

Although front-end preventive controls over the tax-relief application approval and input procedures were present, detective change-control procedures and system capabilities to track unauthorized account modifications could be improved. (§2.1 of Report). The software used for processing tax-relief applications did not provide an audit trail of user modifications to taxpayer records. Tax-relief clerks accepted and reviewed applications for accuracy and completeness. However, this process did not provide adequate internal controls to prevent or mitigate the risk that fraudulent information could be entered in a taxpayer's record and go undetected. The tax relief programs are a challenge to manage and control due to the legacy tax application currently in use by the County. The County will be implementing a new Tax Administration System (CCI *CollectWare*) within the next 18 to 24 months. The new system will provide audit trails. The Treasurer's Office should continue its participation in the system's development group to insure that controls to detect unauthorized changes to a taxpayer's record are adequately addressed with the current tax application.

RECOMMENDATION:

The Treasurer's Office should continue its multi-year efforts with County IS to implement a series of fields in the taxpayers' records that would track the employee who performed each step in the tax-relief application process. This would allow supervisors to detect unauthorized modifications to taxpayers' records.

ACTION TAKEN:

As an interim, partial solution, the Treasurer recently implemented the capture of notes entered into the tax relief application that creates a database of the note, operator ID, and date and time of entry.

ACTION IN PROCESS:

The Treasurer's Office is taking action to validate that the County's new tax administration system has adequate detective change-control capability to mitigate the risk of undetected change to a taxpayer's record.

The County's general-warrant checking account, unlike any other warrant-funding account, consistently had a significant excess balance, which created a risk for misappropriation (§3.1 of Report). The County Treasurer maintained a "reserve" amount in the general warrant checking account in the event of an unanticipated financial crisis or natural disaster. Widely accepted best practices suggest methods of managing cash disbursements and cash account reconciliations. The most common practice suggests that approved cash disbursements should draw the disbursement account to a zero balance. This control on cash disbursements prevents the account from carrying a balance beyond the payment of approved accounts payable (warrants).

RECOMMENDATIONS:

Because there is a demonstrated $3.4 million average monthly float, the Treasurer could fund the general warrant checking account as a zero-balance account.

The Treasurer should consider transferring the "Treasurer's Investment" portion held in the general-warrant checking account into a separate account.

ACTION TAKEN:

In April 2010, the Treasurer's Office transferred $9,000,000, representing the "Treasurer's Investment" portion, out of the general-warrant checking account.

Payment cards were accepted for the settlement of amounts owed on returned checks in violation of the County's payment-card Merchant Agreement (MA) (***§1.6 of Report).*** The Treasurer followed a different interpretation of the contract stipulations of the payment card processor's MA, which we interpreted to specifically forbid the acceptance of payment cards to settle amounts owed on dishonored checks.

After reviewing these MA terms with the Treasurer, he made inquiries with the State's contract provider. The Treasurer was advised that, when the cardholder has specifically authorized the transaction to clear both the returned check, and the returned-check charges and fees levied by the Treasurer; this is deemed a completely separate transaction from the original payment by check to a County agency. Thus, the transaction would not violate the MA terms and conditions.

Our office was not involved in conversations with the State's contract provider and has difficulty relying on an informal interpretation regarding a potentially sensitive legal issue.

RECOMMENDATION:

The County Treasurer should further review the MA Terms and Conditions with the contract provider and obtain a written interpretation of the returned-check issue.

Further training may be necessary for employees responsible for collection activities on dishonored checks.

Refer to Section V for more detailed discussions of these findings, as well as additional findings regarding the Treasurer's Office.

II. Introduction

This section of the report provides an introductory overview of the County Treasurer's operations. As an elected official, the Treasurer is responsible for billing and collecting property taxes levied by all local taxing entities within the County, in addition to Salt Lake County itself. These entities include local cities and townships, school districts, water and improvement districts, unified police and fire agencies, and the like.

To start this process, the Treasurer's Office prepares the annual "tax notices" which are mailed to taxpayers by November 1 each year. Property taxes detailed in the tax notice are due by November 30. After this date, any unpaid property tax becomes delinquent. The office is also tasked with administering statutory tax-relief programs for certain qualified taxpayers within Salt Lake County. As a final step, the Treasurer's Office distributes to the appropriate local taxing entities property taxes collected in compliance with State law.

The Salt Lake County Assessor's Office bills and collects personal property taxes assessed to businesses within the County, and deposits these collections with the Treasurer. State Statute requires the Treasurer to distribute tax collections to all taxing entities by the 10th of each month and to effect a final settlement with these entities by March 31 each year, which details the collections of the prior year.

Motor vehicle fees, sales and use taxes, car rental, and restaurant taxes are examples of taxes and fees collected on behalf of Salt Lake County by the Utah State Tax Commission (Tax Commission). The Treasurer accepts daily direct deposits into a separate Public Treasurer's Investment Fund (PTIF) account for motor vehicle flat fees, age-based fees, and inspection/emission fees. In addition, sales and use taxes as well as car rental and restaurant taxes are deposited directly by the State Tax Commission into the Treasurer's general PTIF account on the last day of each month.

By law, monies collected by County agencies from any source must be deposited into an account under the control of the County Treasurer.

Various County agencies collect user fees and payments for goods and services. These collections are deposited into separate agency depository accounts. The balances of these depository accounts are swept into a bank account under the control of the County Treasurer. Each day, the Treasurer's Office submits a journal voucher to the Auditor's Office, which settles with the County for all departmental receipts. The Treasurer's Office invests all funds deposited in County accounts in accordance with the State Money Management Act.

The Treasurer is also responsible for funding general and payroll warrants issued by the County Auditor. Costs incurred by the County are paid by issuing general warrants and are broken down by each County fund type. The Treasurer reduces the investment portfolio balance to pay these expenses if sufficient daily collections are not available to cover issued warrants. Payroll warrants are funded semi-monthly, and are paid either by

County warrants issued to employees or through direct deposits to individual employee accounts.

At the time of the audit, the Treasurer's Office had 27 full-time equivalent employees who performed cashiering functions, made disbursements, maintained accounting records, and administered statutory programs for tax abatements or exemptions. The Treasurer's General Ledger (TRGL) is used to record accounting entries. The entries are for tax and fee collections and cash flows within Salt Lake County Government.

The scope and objectives of this audit are discussed in the following section.

III. Scope and Objectives

This audit was designed to examine and evaluate the Treasurer's Office system of internal controls and to assess their efficiency and effectiveness in performing the Treasurer's mandated responsibilities. Key areas of evaluation during the audit included:

- Reliability and integrity of information reported by the Treasurer's Office
- Compliance with policies, procedures, laws, regulations, and contracts
- Proper safeguarding of County assets
- Economical and efficient use of County resources
- Accomplishment of established objectives and goals for operations or programs

Our audit work was limited to the period between April 1, 2008 and March 31, 2009. The scope of the audit included an examination of the Treasurer's compliance with Countywide Policies, including Countywide Policy #1062, Management of Public Funds. We also examined the collection and disbursement of property taxes, the management of the County's investment portfolio, the funding of County general and payroll warrants, and the issuance and management of County debt obligations. In addition, we reviewed the Treasurer's role in facilitating the acceptance of payment cards for services, fees, and merchandise sales at various County agencies, and the Treasurer's Office compliance with National Automated Clearing House Association (NACHA) requirements and security standards for accepting electronic property tax payments from taxpayers. Due to certain security issues related to the County's ACH transactions and the role of County Information Services and other County agencies in these matters, information regarding ACH transactions was not included in this report. Audit matters regarding information systems security are protected under the Government Records Access Management Act (GRAMMA) § 63-2-304. The users of this report should note that we did not examine all areas of the Treasurer's Office operations.

The principal objectives of the audit were to:

- Obtain an understanding of the duties and responsibilities of the Treasurer's Office as described in Utah Code Annotated (UCA) §17-24-1
- Assess the operational risks inherent in carrying out the key business functions of the Treasurer's Office
- Identify the internal controls established to manage those operational risks and to test those controls in order to ensure that they are functioning properly in the manner in which they were designed

- Identify and recommend potential improvements to the Treasurer's key business processes, and where appropriate, recommend ways in which to tighten internal control procedures, and improve operational efficiency and effectiveness
- Add value to the Treasurer's Office operations by providing an audit report that is useful to management

IV. Summary of Findings and Recommendations

#	Findings	Recommendations	Reference Page
1.0	**Administration**		**13**
1.1	Cashiering system totals were not compared to cash/check exchange transaction totals at the time each change fund replenishment request was prepared.	The cash/check exchange transaction totals obtained from the iNovah cashiering system could be used to determine the amounts included in the change fund replenishment requests.	14
1.2	A portion of the petty cash fund was converted into an imprest checking account, without following the steps required by Countywide Policy to first obtain approval from the Auditor and Mayor.	The Treasurer's Office should close the imprest checking account and use its purchasing card to facilitate small-dollar purchases of over-the-counter items. If the first recommendation is not implemented, the Petty Cash Fund Custodian should coordinate with the Auditor's Office to properly establish an imprest checking account to make small-dollar purchases of over-the-counter items, but not for some of the purposes for which the petty cash funds were used in the past.	17
1.3	The petty cash fund was too large for its actual level of utilization.	The petty cash fund balance should be reduced to a level more appropriate to the Treasurer's Office operational needs.	19
1.4	The Treasurer's Office had several commendable capital and controlled asset management practices.	COMMENDATION: The Treasurer's Office is to be commended for addressing risks and putting into place several positive asset-management practices.	19

#	Findings	Recommendations	Reference Page
1.5	The Pelco video recorder system was not properly identified on the Treasurer's Office capital asset inventory list.	The Treasurer's Office Property Manager should complete a Salt Lake County Property Transfer/Disposal/Internal Sale Form PM-2, to transfer the records of the Pelco video recorder system from County Facilities to the Treasurer's Office. In doing so, the location and asset description can be updated and included on the Treasurer's Office capital asset listing to ensure proper identification and accounting for the system. ACTION TAKEN: In December 2009, a Salt Lake County Property Transfer/Disposal/Internal Sale Form PM-2 was submitted to the Auditor's Office from County Facilities to transfer the ownership of the Pelco video recorder system to the Treasurer's Office.	21
1.6	Payment cards were accepted for the settlement of amounts owed on returned checks in violation of the County's payment-card Merchant Agreement.	The County Treasurer should further review the MA Terms and Conditions with the contract provider and obtain a written interpretation of the returned-check issue. Further training may be necessary for employees responsible for collection activities on dishonored checks.	22
1.7	County agency fiscal managers and fiscal personnel were not given adequate information with respect to the County's payment card Merchant Agreement and PCI Data Security Standards.	The Treasurer, as Chair of the Fund Management Policy Committee, and with the support of the Employees' University, should develop and implement training for fiscal personnel on the requirements of the MA Terms and Conditions and PCI DSS. The Treasurer should take a pro-active role in carrying out his duties and responsibilities set forth in Countywide Policy #1062, Section 1.11 and Section 2.8.1, or work to change or rescind the policy provisions. ACTION TAKEN: The Treasurer's Office is currently an active participant in an ad hoc committee formed to review and determine PCI DSS compliance requirements and to formulate Countywide Policy to provide guidance to County Agency Managers.	25

#	Findings	Recommendations	Reference Page
2.0	**Collections**		**29**
2.1	Although front-end preventive controls over the tax-relief application approval and input procedures were present, detective change-control procedures and system capabilities to track unauthorized account modifications could be improved.	The Treasurer's Office should continue its multi-year efforts with County IS to implement a series of fields in the taxpayers' records that would track the employee who performed each step in the tax-relief application process. This would allow supervisors to detect unauthorized modifications to taxpayers' records. ACTION TAKEN: As an interim, partial solution, the Treasurer recently implemented the capture of notes entered into the tax relief application that creates a database of the note, operator ID, and date and time of entry. ACTION IN PROCESS: The Treasurer's Office is taking action to validate that the County's new tax administration system has adequate detective change-control capability to mitigate the risk of undetected change to a taxpayer's record.	30
3.0	**Accounting**		**32**
3.1	The County's general-warrant checking account, unlike any other warrant-funding account, consistently had a significant excess balance, which created a risk for misappropriation.	Because there is a demonstrated $3.4 million average monthly float, the Treasurer could fund the general warrant checking account as a zero-balance account. The Treasurer should consider transferring the "Treasurer's Investment" portion held in the general-warrant checking account into a separate account. ACTION TAKEN: In April 2010, the Treasurer's Office transferred $9,000,000, representing the "Treasurer's Investment" portion, out of the general-warrant checking account.	35

V. Findings and Recommendations

For the purposes of this report, findings and recommendations have been divided into the following three sections:

- Administration
- Collections
- Accounting

These sections correspond to the general operational areas and divisions within the Treasurer's Office and are described below.

Administration. Findings and recommendations in the Administration area included results from our examination of imprest funds such as petty cash and the Treasurer's Office change fund, capital and controlled asset management, and other administrative duties and responsibilities of the Treasurer's Office.

Collections. The Collections Division of the Treasurer's Office is responsible for the collection of real property taxes and related charges due to Salt Lake County and all other taxing entities within the County. Besides processing payments and performing the actual cashiering duties of collecting real property taxes due from taxpayers, the Collections Division also includes sections devoted to redemption of taxes receivable, facilitation of property tax liens, and administration of statutory tax relief programs.

Accounting. The Accounting Division reconciles collections and distributes tax revenues to all taxing entities within Salt Lake County, including the various County agencies themselves. The Accounting Division is responsible for managing the County's investment portfolio, funding warrants issued by the Auditor's Office, implementing state and board of equalization ordered adjustments and refunds, and refunding tax overpayments. Additionally, the Accounting Division is responsible for annually reporting to the Tax Commission and to tax entities.

1.0 Administration

The County Treasurer engages in several administrative activities required to carry out the Treasurer's statutory duties of collecting and distributing property taxes and fees to all taxing entities within Salt Lake County. For example, the Treasurer maintains a change fund for cashiering purposes when collecting real property tax payments from taxpayers. Likewise, a petty cash fund has been established for making small purchases essential to day-to-day operations. County assets used by Treasurer's Office employees in the performance of their duties must also be properly accounted for and safeguarded. County policy requires the Treasurer to attempt collection on returned checks for most County agencies, as well.

For the purposes of this report, we have categorized these types of administrative duties and activities separately from the other two categories, Collections and Accounting, to organize the information presented in a logical and systematic format. As an elected County Official, the volume and complexities of transactions presented to the Treasurer on a daily basis, in performing the Treasurer's statutory duties and administrating a County office are varied, and often quite challenging. The user of this report should not infer that our review and findings in this area are all-inclusive, or address every possible area of risk. Our findings in this area are as follows:

- ***Cashiering system totals were not compared to cash/check exchange transaction totals at the time each change fund replenishment request was prepared.***
- ***A portion of the petty cash fund was converted to an imprest checking account, without following the steps required by Countywide Policy to first obtain approval from the Auditor and Mayor.***
- ***The petty cash fund was too large for its actual level of utilization.***
- ***The Treasurer's Office had several commendable capital and controlled asset management practices.***
- ***The Pelco video recorder system was not properly identified on the Treasurer's Office capital asset inventory list.***
- ***Payment cards were accepted for the settlement of amounts owed on returned checks in violation of the County's payment-card Merchant Agreement.***
- ***County agency fiscal managers and fiscal personnel were not given adequate information with respect to the County's payment card Merchant Agreement and PCI Data Security Standards.***

1.1 Cashiering system totals were not compared to cash/check exchange transaction totals at the time each change fund replenishment request was prepared.

The Treasurer's Office maintains a change fund for cashiering purposes when collecting payments on real property taxes due from taxpayers. Treasurer's Office cashiers are authorized to cash personal and payroll checks from Salt Lake County employees from this fund, as well. The Treasurer's Office change fund is unique in that it is:

- Not restricted from cashing County employee personal checks
- Not replenished by a warrant issued from the Auditor's Office, as are other County agency change funds

For each cash/check exchange transaction, Treasurer's Office cashiers complete a Cash/Check Exchange Form, enter the transaction into the iNovah cashiering system, and disburse cash from the change fund. When cash is depleted, a Change Order Request Form is completed, normally twice a month, to place a request with the bank to replenish the change fund.

Supporting documentation attached to each Change Order Request includes the pink copies from the 3-part Cash/Check Exchange Forms completed by the cashiers for each cash/check exchange transaction. The completed Change Order Request is reviewed by the Deputy Treasurer for accuracy, and the pink copies are examined for any suspicious entries or alterations. Once approved by the Deputy Treasurer, the information from the Change Order Request is used to place a change order online.

Due to timing differences, Change Order Request amounts did not match reported cash/check exchange transaction totals obtained from the cashiering system.

Our audit procedures included an examination of a sample of 24 Change Order Requests, and the supporting documentation. We obtained a report from the iNovah cashiering system detailing cash/check exchange transactions entered over the same time period for each change fund replenishment request. In 12 out of 24 instances, we found that the Change Order Request amounts included Cash/Check Exchange Forms (pink forms) which were dated from a prior replenishment request period.

This overlap was created by the daily cutoff of transactions in the iNovah system, and, in some cases, were the result of holiday periods during which the Treasurer's Office was closed. Table 1 on page 16 shows the timing differences between the dates and amounts of the Change Order Requests and the monthly cashiering-system totals as recorded in iNovah. Dates highlighted in red, show an overlap of beginning and ending dates of change order requests during the audit period. The table also illustrates the timing differences between the iNovah system report cutoff dates and the dates on which change fund replenishment requests were prepared.

Differences Between iNovah System Reports and Change Fund Replenishments						
iNovah Allocation Reports			Change Order Request Forms			Difference
Beginning Date	Ending Date	Total Amount	Beg. Dates (Pink Copies)	End. Dates (Pink Copies)	Change Order Totals	Between Reports/Forms
4/1/2008	4/30/2008	$ 31,655.80	4/1/2008	4/18/2008	$ 25,970.00	$ (5,685.80)
5/1/2008	5/31/2008	30,850.18	4/18/2008	5/9/2008	21,044.00	(9,806.18)
6/1/2008	6/30/2008	28,417.61	5/14/2008	6/20/2008	39,510.00	11,092.39
7/1/2008	7/31/2008	28,997.68	6/20/2008	7/21/2008	27,337.00	(1,660.68)
8/1/2008	8/31/2008	34,208.98	7/15/2008	8/27/2008	35,101.00	892.02
9/1/2008	9/30/2008	38,672.45	8/20/2008	9/22/2008	39,634.00	961.55
10/1/2008	10/31/2008	35,804.63	9/19/2008	10/20/2008	32,865.00	(2,939.63)
11/1/2008	11/30/2008	36,006.96	10/20/2008	11/21/2008	35,220.00	(786.96)
12/1/2008	12/31/2008	36,786.87	11/20/2008	12/19/2008	37,379.00	592.13
1/1/2009	1/31/2009	33,699.81	12/19/2008	1/23/2009	33,658.00	(41.81)
2/1/2009	2/28/2009	35,900.63	1/20/2009	2/20/2009	38,189.00	2,288.37
3/1/2009	3/31/2009	40,720.12	2/20/2009	3/31/2009	44,923.00	4,202.88
Total		**$411,721.72**	**Total**		**$ 410,830.00**	**$ (891.72)**

Table 1. ***Differences between cash/check exchange transactions recorded in the iNovah cashiering system compared to Change Order Request Form totals.***

The Treasurer's Office prepares change fund replenishment requests using a pre-determined amount. As a result, the Head Cashier and Collections Director routinely exclude some pink forms, which would normally fall into the cut-off period when preparing a change fund replenishment request. Without a strict cut-off of dates for pink forms in the replenishment request, the totals from the cash register system for a specific time period would not match the total of the replenishment request for the same time period.

After discussing this observation with the Treasurer, he provided a complete reconciliation between the iNovah system report totals and the Change Order Request totals during the period we reviewed. Because the change fund is only replenished when needed and the iNovah system is balanced and closed daily, an overlap between cashiering system transaction dates and replenishment request dates occurs. However, Change Order Request amounts could be determined from the iNovah cashiering system reports eliminating the need to tally separate pink forms.

When a replenishment request is prepared, all the pink forms within the date range specified on the iNovah cashiering system report should be included in the request. This would reduce the risk that a fraudulent pink form could be created or an existing one altered and not be detected.

All transactions entered into the iNovah system are posted to the Treasurer's General Ledger (TRGL). In addition, as an internal control procedure, the change fund balance is reconciled with the ledger balance of the account in the TRGL. During our review, we noted that timing differences between the transactions entered into the iNovah cashiering system and the documentation included with the Change Order Request Forms could be reconciled more easily using transaction reports generated directly from the iNovah system.

As an additional internal control procedure over the change fund balance, transaction summary reports could be generated by the iNovah system which correspond to a given date range of a specific Change Order Request. Any timing differences between the Change Order Request and the iNovah system report could be quickly identified and used as an additional means to assure that the change fund balance is true and accurate.

Countywide Policy #1203, "Petty Cash and Other Imprest Funds," requires that change fund custodians and their supervisors be responsible for properly managing and accounting for funds under their control. This change fund's unique purpose and direct-bank replenishment procedures require, in our opinion, even greater intra-agency controls over reconciliation procedures, since Treasurer's Office employees operate, balance, and replenish the fund themselves, without, for example, issuance of a warrant by the Auditor's Office.

RECOMMENDATION:

The cash/check exchange transaction totals obtained from the iNovah cashiering system could be used to determine the amounts included in the change fund replenishment requests.

1.2 A portion of the petty cash fund was converted to an imprest checking account, without following the steps required by Countywide Policy to first obtain approval from the Auditor and Mayor.

Our audit procedures included an unannounced count of petty cash funds and a review of petty cash disbursements. During the surprise count, we discovered that the Treasurer's Office had converted a majority of their petty cash fund into a checking account held at Wells Fargo Bank. We obtained the Salt Lake County Petty Cash and Other Imprest Accounts listing from the County Auditor's Office and verified that the Treasurer's Office petty cash fund had an authorized balance of $500, and that it was recorded as a "cash-only" fund type. The imprest checking account did not appear on this list of approved accounts. Our count revealed that the actual cash on hand in the petty cash fund was only $4.98. The remainder of the authorized balance was either deposited in the checking account, or was documented with petty cash vouchers as cash or check disbursements.

The Treasurer's Office used the checking account to pay for items purchased and invoiced through the mail.

After reviewing petty cash vouchers and receipts for disbursements, we determined that the Treasurer's Office used the checking account to pay for items purchased and invoiced through the mail, such as magazine subscriptions and office nameplates. In a few instances, purchases were made in excess of the $200 petty cash spending limit.

Countywide Policy #1203, “Petty Cash and Other Imprest Accounts,” Section 3.5, states:

> *"Disbursements from petty cash...are for the purpose of covering over-the-counter, cash purchases under the specified limit...the items purchased shall be paid for at the time of the transaction. Any purchases "charged" with a vendor under the County's credit are to be processed under established accounts payable procedures, and not subsequently paid from a petty cash or other imprest account. To do otherwise is in conflict with the purpose of this policy and is considered to be not cost effective."*

Countywide Policy #1203 differentiates between the purposes and intent of petty cash funds as opposed to imprest funds. As stated in Countywide Policy #1203, “Petty Cash and Other Imprest Accounts,” Sections 1.2 and 1.4, the definitions of a petty cash fund and an imprest checking account are as follows:

> *”Petty Cash Fund – an amount of cash available for small purchases relating to normal business operations.*
>
> *Imprest Checking Account – an amount of cash available in an established commercial bank for purposes similar to petty cash funds, but which is generally established in larger imprest amounts. A reasonable portion of this amount (in most cases not to exceed $200) may be maintained in cash to accommodate small cash transactions.”*

Additionally, the procedures to establish an imprest fund are outlined in Countywide Policy #1203, Section 2.0. These procedures include forwarding an MPF Form 2 to the Accounting and Operations Division of the Auditor’s Office requesting the establishment of the imprest fund.

RECOMMENDATIONS:

The Treasurer’s Office should close the imprest checking account and use its purchasing card to facilitate small-dollar purchases of over-the-counter items.

If the first recommendation is not implemented, the Petty Cash Fund Custodian should coordinate with the Auditor's Office to properly establish an imprest checking account to make small-dollar purchases of over-the-counter items, but not for some of the purposes for which the petty cash funds were used in the past.

1.3 The petty cash fund was too large for its actual level of utilization.

As stated above, the Treasurer's Office had an authorized petty cash fund balance of $500. At the time of our surprise count, the petty cash fund balance had $4.98 cash on hand, $241.62 deposited in the checking account, with the remainder of $253.40 expended through cash or check disbursements. We obtained petty cash fund replenishment records from the Auditor's Office to analyze the use of the authorized balance of this petty cash fund, and the types and amounts of disbursements. During 2008, the petty cash fund was only replenished twice, once on March 13, 2008 for $421.00 and again on October 3, 2008 for $401.07. The total petty cash funds disbursed during 2008 was $822.07.

During 2008, the petty cash fund was only replenished twice.

Countywide Policy #1203, "Petty Cash and Other Imprest Accounts," Section 3.7, states:

> *"The amount requested shall provide adequate operating funds for approximately three (3) months."*

The amount of petty cash funds used in 2008 divided by four is only $205.52 (if the fund had been replenished every three months). Since the current authorized balance of the Treasurer's Office petty cash fund is $500, the petty cash fund could be over-funded by almost $300 ($500 - $206), based on the level of use in 2008.

Because some of the petty cash fund balance remains idle, unused funds lose potential interest earnings or could be appropriated to other areas of need within the County. Based on current criteria, the Treasurer's Office petty cash fund balance is too large for its current turnover, as outlined in Countywide Policy #1203.

***RECOMMENDATION*:**

The petty cash fund balance should be reduced to a level more appropriate to the Treasurer's Office operational needs.

1.4 The Treasurer's Office had several commendable capital and controlled asset management practices.

Our audit procedures also addressed the risk that County assets acquired and in use in the Treasurer's Office might not be properly safeguarded and/or accounted for. Assets that are not properly safeguarded or accounted for could be lost, stolen, or converted to personal use by County employees.

Countywide Policy #1125, "Safeguarding Property/Assets," distinguishes between "capital" and "controlled" assets as follows:

- *Capital Asset. An individual item having an estimated useful life exceeding one year and a cost equal to or greater than the capitalization rate defined in County ordinance, currently $5,000.*

- *Controlled Asset. An item of personal property having a cost of $100 or greater, but less than the current capitalization rate. These assets, such as cell phones, desk/laptop computers, etc., are easily converted to personal use, and therefore require special provisions for tracking and safeguarding. Regardless of cost, personal electronic communications equipment items are always considered controlled assets due to the difficulty associated with establishing centralized control over these assets.*

During our testing of compliance with Countywide Policy #1125, we found several positive asset-management practices in place within the Treasurer's Office, which included:

The Treasurer's Office is to be commended for establishing a sound asset-management control environment.

- *Unique ID number tags on both capital and controlled assets to allow better asset inventory control and easier identification.*

- *Complete capital and controlled asset inventory lists, which include ID number tags, asset descriptions, model numbers, serial numbers, dates placed in service, and location descriptions for each asset.*

- *An office policy, which requires an annual inspection and inventory of all capital and controlled asset items. The most recent controlled asset inspection at the time of the audit was November 24, 2008.*

- *Proper storage and physical safeguards in place for capital and controlled assets, which are susceptible to theft or conversion to personal use.*

These practices foster a sound asset-management control environment and greatly reduce the risk that County assets could become lost, stolen, or converted to personal use. The Treasurer's Office is to be commended for putting these practices in place and addressing these risks.

COMMENDATION:

The Treasurer's Office is to be commended for addressing risks and putting into place several positive asset-management practices.

1.5 The Pelco video recorder system was not properly identified on the Treasurer's Office capital asset inventory list.

Our audit procedures included examining a random sample of both capital and controlled assets. An inventory was completed of the sample items, and the results were compared with the Treasurer's Office capital and controlled asset listings and the Capital Asset Inventory Listing by Organization report (AFIN0801) obtained from the County Auditor's Capital Assets Section.

A Pelco brand video recorder system was not listed on the Treasurer's Office capital asset listing.

During our asset inventory, we discovered a Pelco brand video recorder system, which was not listed on the Treasurer's Office capital asset listing or on the Capital Asset Inventory Listing by Organization report (AFIN0801). The Treasurer's Property Manager stated that Salt Lake County Facilities had purchased and installed the video recorder system, and, therefore, maintained the asset record for that item. To verify this, we asked County Facilities' management about the accounting for the video recorder system.

County Facilities had originally purchased and installed the Pelco video recorder system as the Treasurer's Property Manager had stated. However, the Treasurer's Office had subsequently paid County Facilities for the system, but did not report the purchase to the Treasurer's Property Manager or the Auditor's Capital Assets Division. Therefore, the transfer of the video recorder system was not reported on a Form PM-2, nor included on the Treasurer's capital asset listing, or the Auditor's capital asset records.

Countywide Policy #1125, "Safeguarding Property/Assets," Section 2.2.3, states that County organizations are responsible for:

> *"Maintain[ing] records as to current physical location of all fixed [capital] assets and controlled assets within the organization's operational and/or physical custody."*

Section 2.2.5 states that each County organization is required to:

> *"Prepare "Salt Lake County Personal Property Transfer/Disposal/Internal Sale Form PM-2" in advance for all fixed asset property transfers, disposal or sales between the Property Manager's organization and any other organization. Research is to be performed if necessary to identify and report the correct fixed asset (tag) number on the PM-2 form."*

A copy of Salt Lake County Personal Property Transfer/Disposal/Internal Sale Form PM-2 is attached as Appendix A.

Capital and/or controlled assets which are not properly identified or accounted for are placed at a greater risk for being misappropriated, lost, or not depreciated properly.

***RECOMMENDATION*:**

The Treasurer's Office Property Manager should complete a Salt Lake County Property Transfer/Disposal/Internal Sale Form PM-2, to transfer the records of the Pelco video recorder system from County Facilities to the Treasurer's Office. In doing so, the location and asset description can be updated and included on the Treasurer's Office capital asset listing to ensure proper identification and accounting for the system.

ACTION TAKEN:

In December 2009, a Salt Lake County Property Transfer/Disposal/Internal Sale Form PM-2 was submitted to the Auditor's Office from County Facilities to transfer the ownership of the Pelco video recorder system to the Treasurer's Office.

1.6 Payment cards were accepted for the settlement of amounts owed on returned checks in violation of the County's payment-card Merchant Agreement.

Many County agencies accept credit and/or debit cards (payment cards) for payment of services, fees, and merchandise sales at locations throughout the County. The Treasurer's Office is responsible for facilitating this process and directs County agencies on where to obtain any needed equipment, and establishes the agency's depository accounts into which the payments are transferred after processing. As the facilitator of this process, the Treasurer maintains the written agreement between the payment-card processor and the County itself. This written agreement is commonly termed the "Merchant Agreement," and is made between the payment-card processor and the merchant, in this case the County, as a whole.

Our audit objectives included a review of the Treasurer's role in establishing the depository accounts for the various County agencies, managing the Merchant Agreement between the agencies and the payment-card processor, and understanding and complying with contract provisions governing payment-card acceptance, processing, and security of cardholder data.

We obtained current copies of both the *Terms and Conditions for Merchant Agreement (Government Entity) Doc 11820 Rev 12/06 (MA Terms and Conditions)*, and the *Merchant Operating Guide (Operating Guide) Rev 09/08*, from the Treasurer. (Copies of these documents are

attached as Appendices B and C. The MA Terms and Conditions agreement is between the payment-card processor and Salt Lake County, and details the applicable criteria and requirements for the proper acceptance of payment cards at all County merchant locations.

We also obtained a listing of all depository accounts, which had been established for the various County agencies that were authorized to accept payment cards. The Treasurer maintains this listing and manages the opening or closing of these accounts.

Countywide Policy #1062, "Management of Public Funds," Section 1.16, defines a merchant agreement as:

The Treasurer established a merchant account for his office to allow acceptance of payment cards from debtors on amounts due resulting from returned checks.

"A written agreement between a bank and a merchant (i.e., the County) setting forth terms, guidelines and standards whereby the merchant agrees to honor all valid bank cards presented as payment for services, products or events and the bank agrees to accept valid sales drafts or transaction records presented for payment."

During our review of the MA Terms and Conditions and the depository account listing maintained by the Treasurer's Office, we noted that the Treasurer established a merchant account for his office to allow acceptance of payment cards from debtors on amounts due resulting from returned checks.

Countywide Policy #1306, "Collection of Bad Checks," Section 2.1, states:

> *"The Salt Lake County Treasurer's office shall attempt collection of all returned checks for all County Agencies."*

Checks written to a County agency that are dishonored for any reason are received by the Treasurer's Office to attempt collection. The recovery of debts owed to Salt Lake County is the responsibility of the County Attorney, but at the Attorney's discretion, some of the collection responsibilities may be delegated to other offices, agencies, or contractors.

In accordance with Countywide Policy #1306, the County Treasurer has the responsibility to attempt initial collection of returned checks for most County agencies except in certain instances outlined in County policy. To aid in the Treasurer's collection efforts, a merchant account was established and a payment-card machine was installed to allow debtors to settle the amount due on dishonored checks by use of their payment card.

As outlined in Countywide Policy #1306, upon notification that a check has been dishonored, the Treasurer will mail a Notice of Returned Check to the debtor. If the debtor fails to respond within 15 days of the first notice, a Second Notice of Returned Check is sent which informs the debtor of legal follow-up. If no response is received 15 days after the

second notice is sent, the matter is turned over to the District Attorney's Office for legal action.

To expedite the initial collections process, the Treasurer allowed amounts owed to the County resulting from dishonored checks to be settled via payment card through the Treasurer's merchant account. We discussed the process with Treasurer's Office employees and determined that, although the use of payment cards to settle dishonored checks was infrequent, it was an established practice offered as an alternative method of payment after the initial Notice of Returned Check had been sent. Therefore, we concluded that, due to the infrequent acceptance of payment cards, the MA Terms and Conditions was not carefully reviewed regarding the prohibition against use of payment cards to settle amounts owed on dishonored checks.

The practice of accepting payment cards for settlement of dishonored checks violates the Merchant Agreement.

As part of our review, we discovered that the practice of collections of returned or dishonored checks via payment card was in violation of the *MA Terms and Conditions*. The *MA Terms and Conditions* (Government Entity) Doc 11820 Rev 12/06, Section 1.4 (3), "Requirements for Sales Data," states:

> *"The **Sales Data** does not involve **any element** of credit for payment of a previously dishonored check or for any other purpose except payment for a current transaction and, except in the case of approved installment or pre-payment plans, the goods have been shipped or services actually rendered to the cardholder." (Emphasis added)*

As defined in Section 17.11, "Definitions," ***Sales Data*** is:

> *"The evidence and electronic record of a sale or lease transaction representing payment by use of a Card or of a refund/credit to a Cardholder."*

After reviewing these MA terms with the Treasurer, he made inquiries with the State's contract provider. He was told that the above quoted provisions in the MA were intended to prohibit automatic charging of a credit card for a returned check.

However, the Treasurer was advised that when the cardholder has specifically authorized the transaction to clear both the returned check and the returned-check charges and fees, levied by the Treasurer; this is deemed a completely separate transaction from the original payment by check to a County agency. According to the contract provider, as long as the cardholder specifically authorizes the charge by the Treasurer, the contract provider is not concerned. Our office would welcome written documentation from the State's contract provider of this interpretation, since it does not follow a stricter interpretation of the MA terms and conditions.

By accepting payment cards to settle dishonored checks, the risk of collections is transferred to the payment-card issuer in violation of the MA Terms and Conditions, and places the County at risk for corrective action by the payment-card processor. Examples of corrective action could include chargebacks for all invalid payments processed, or termination of the merchant agreement as outlined in the contract under Section 7, "Chargebacks," and Section 10 "Termination." Not only would these actions affect the Treasurer's Office merchant account, but all other County agencies currently bound by the *MA Terms and Conditions*.

***RECOMMENDATION*:**

The County Treasurer should further review the MA Terms and Conditions with the contract provider and obtain a written interpretation of the returned-check issue.

Further training may be necessary for employees responsible for collection activities on dishonored checks.

1.7 County agency fiscal managers and fiscal personnel were not given adequate information with respect to the County's payment card Merchant Agreement and PCI Data Security Standards.

As previously noted, the Treasurer's Office has sole authority to establish bank accounts. In addition, the Treasurer's Office facilitates the establishment of merchant card locations, and coordinates acquisition of payment-card processing machines for all County agencies. At the time of this writing, the County had 89 agencies that used onsite payment-card machines. We also noted that 24 agencies accepted web-based payment-card transactions.

To determine payment-card usage trends for Salt Lake County, we obtained the only comparable data available from the Utah State Purchasing and General Services Division. To identify usage trends, we compared data from the second quarters of 2006, 2007, and 2008. The increased usage demonstrates greater reliance on the County's acceptance of payment cards, and thus a greater need for training of fiscal personnel. Table 2 below shows the increased trend in the use of payment cards in the County.

Salt Lake County Payment Card Trends					
	Sales	**Refunds**	**Net Sales**	**Transactions**	**Change**
2nd Qtr 2006	$3,144,213	-$29,714	$3,114,499	79,779	n/a
2nd Qtr 2007	$5,520,248	-$42,481	$5,477,767	116,325	+46%
2nd Qtr 2008	$5,851,173	-$90,496	$5,760,677	125,731	+8%

Table 2. ***Payment card trends for the 2nd Quarters of 2006-2008.***

The MA Terms and Conditions set out specific requirements for the acceptance of these transactions. They include the following procedures:

- Retention of cardholder data
- Restrictions on transaction types
- Issuance and security of receipts
- Consequences of chargebacks
- Settlement by next business day
- Issuance of refunds

The PCI DSS establishes 12 requirements that address security over the acceptance of payment cards at the point of sale, over the internet, via phone, or through the mail. These requirements range from encryption of transmitted payment-card data to storage and retention of receipts. The County's payment-card processor was certified by an independent Qualified Security Assessor (QSA) as PCI DSS compliant as of May 1, 2009 for the Visa payment-card brand. This certification was verified on Visa's Global List of PCI DSS Validated Service Providers. The Global List appears in this report as Appendix D.

PCI DSS requirement #'s 7, 8, and, 9 are directly applicable to County agencies who accept payment cards. These requirements provide guidance on access control measures such as:

- Requirement # 7 - Restricting access to cardholder data based on business-related need-to-know
- Requirement # 8 - Assigning a unique ID to each person with computer access
- Requirement # 9 - Restricting physical access to cardholder data

Countywide Policy #1062, Management of Public Funds, establishes the Treasurer's Office as the central authority responsible for cashier training and establishment of agency payment-card accounts. However, the policy is silent regarding the important issue of training fiscal personnel on the provisions of the MA Terms and Conditions and PCI DSS requirements. Cited below are the provisions of Policy #1062 relevant to the Treasurer's role in development of fund management policy, protocol, procedure, or amendments thereto.

Countywide Policy #1062, Section 1.11, states that the Fund Management Policy Committee, chaired by the Treasurer,

> *"…shall meet as needed and shall have responsibility for **developing, reviewing, and making recommendations** to the Mayor or Council on any proposed fund management policy, protocol, procedure, or amendment thereto. The committee, through its Chair, shall be responsible for providing clarification*

and guidance with respect to the interpretations of fund management policies." (Emphasis added)

However, the Fund Management Policy Committee has been inactive for a number of years. Based on our assessment of the overall control environment with regard to payment-card transactions, we concluded that the Treasurer has been challenged in keeping abreast of developments regarding the increased use of payment cards and the inherent risks involved in these transactions.

Countywide Policy #1062, Section 2.8.1, also states:

"Treasurer may review cash handling practices, books, papers, and accounts to ensure compliance with state law and this policy, and to identify possible improvements in cash handling."

This section of County policy encourages the Treasurer to review cash handling practices for compliance with State law. We recognize that PCI DSS requirements and MA Terms and Conditions do not fall under the purview of State law, however, the spirit of Policy #1062 charges the Treasurer with an active role in ongoing development and modification of funds management policies, procedures, and training to include industry-developed standards and related requirements.

Moreover, violation of these standards could have significant negative consequences to the County, such as:

- Revocation of payment-card processor's merchant agreement
- Significant chargebacks
- Compromise or loss of cardholder personal identifiers
- Adverse publicity to the County with respect to any of the above
- Substantial penalties at the Federal level for disclosure of personal identifiers

Countywide Policy #1062, Section 3.14.1 – 3 states:

"Any agency authorized to accept credit [payment] cards as payment for County services, products or events must contact the County Treasurer for account preparation. Account preparation includes assigning a Merchant Identification Number to the agency. The Treasurer will refer the agency to the appropriate depository bank to obtain the Merchant Identification Number for the agency.

It is the responsibility of the County Agency to purchase or lease credit [payment] card equipment. It is the responsibility of the County Agency to process credit [payment] card transactions in accordance with the Merchant Operating Manual provided by the processing bank."

Even though the current Merchant Operating Manual advises merchants (County Agencies) to be aware of PCI DSS requirements, the cited policy section does not make specific reference to PCI DSS provisions. This leaves each County Agency with the formidable task of being aware of, understanding, and training their fiscal staff on complex requirements of PCI DSS.

We verified with the Treasurer that PCI DSS provisions, including cardholder-data security standards, are not included in training of County fiscal management or staff, including cashiers. During our interviews, the Treasurer stated that it is not his responsibility to provide this training. This, again, does not seem to be in the spirit of the provisions of Countywide Policy #1062, Section 1.11.

Fiscal personnel were not trained in cardholder data security.

In our audits throughout the County, fiscal personnel, with few exceptions, do not understand the application of the *MA Terms and Conditions* or *PCI DSS requirements* for day-to-day transactions. Training will raise awareness of controls and encourage personnel to review and implement necessary safeguards.

In the absence of awareness training, the risk of violating the merchant agreement or compromising cardholder data, particularly personal identifiers, will not be mitigated and could subject the County to substantial fines and penalties.

***RECOMMENDATION*:**

The Treasurer, as Chair of the Fund Management Policy Committee, and with the support of the Employees' University, should develop and implement training for fiscal personnel on the requirements of the MA Terms and Conditions and PCI DSS.

The Treasurer should take a pro-active role in carrying out his duties and responsibilities set forth in Countywide Policy #1062, Section 1.11 and Section 2.8.1, or work to change or rescind the policy provisions.

ACTION TAKEN:

The Treasurer's Office is currently an active participant in an ad hoc committee formed to review and determine PCI DSS compliance requirements and to formulate Countywide Policy to provide guidance to County Agency Managers.

2.0 Collections

The Collections Division is responsible for the collection of real property taxes and related charges due Salt Lake County and all other taxing entities within the County. To accomplish its objectives, the division is divided into four sections: Accounts Receivable, Tax Relief, Property Liens, and Cashiering.

Accounts Receivable. The Accounts Receivable section administers the collection of both current and delinquent property taxes and maintains taxpayer account records. Changes in mailing addresses, mortgage holder information, or any other taxpayer-account information are updated by the Accounts Receivable section in the County's Property Tax System.

Tax Relief. The Tax Relief section is responsible for administering the various statutory tax relief programs in Salt Lake County. Annual applications for tax relief are received, reviewed, and processed by this section, prior to awarding relief to taxpayers based on need, disability, or financial hardship. These include the following tax relief programs:

- Circuit Breaker Tax Abatement
- Indigent or Hardship Abatement
- Disabled Veteran's Exemption
- Blind Person's Exemption

These programs are made available to taxpayers who meet the minimum requirements for a property tax adjustment, as determined by State and Federal law.

Property Liens. The Property Liens section is responsible for administering property tax liens against centrally-assessed County property (State-assessed property), properties under the protection of the Bankruptcy Courts, and various other non-County assessed properties; or, combinations of tax liens against properties where an ownership change has occurred, or the existing legal property description changed.

Cashiering. The Cashiering section is responsible for processing all real-property-tax monies paid to the County, and for administering the property tax prepayment program.

We noted the competency and professionalism of the Collections Division employees in performing their duties and responsibilities, especially during peak property tax collection periods related to statutory, tax-payment due dates. We commend them on the exemplary way they perform this vital work.

In performing our audit tests, we found some areas where operational efficiency could be improved, and internal controls could be strengthened. Our findings in the Collections area are as follows:

- ***Although front-end preventive controls over the tax-relief application approval and input procedures were present, detective change-control procedures and system capabilities to track unauthorized account modifications could be improved.***

2.1 Although front-end preventive controls over the tax-relief application approval and input procedures were present, detective change-control procedures and system capabilities to track unauthorized account modifications could be improved.

Our audit objective in this area included a review and examination of the process of governing the administration of statutory tax-relief programs by the Collections Division, Tax-Relief Section.

We discovered that there were not adequate internal controls over the input of tax-relief application information into the tax system. We reviewed with the Deputy Treasurer and Collections Director the internal control procedures in place to prevent a tax-relief clerk from entering false information into a taxpayer's account if a paper application was not submitted to authorize the change. We discovered, and management agreed, there were no internal controls to prevent this from happening.

Each year a tax-relief application is prepared and submitted by the taxpayer. Once received by the Treasurer's Office, the form was rigorously screened through a series of audits performed by different tax-relief personnel. As expected, the screening process was focused on a review of information submitted on the application and the supporting documentation. Finally, there was an initial, one-time review of whether information entered into the system from the application was complete and accurate.

An audit trail did not exist to show modifications to taxpayer records.

However, because the software used for processing tax-relief applications did not provide an audit trail, there was no way of tracking in the system any subsequent taxpayer-record modifications. The absence of a taxpayer record access detection control could result in subsequent, undetectable modification of a record granting unwarranted tax relief.

Currently, a tax-relief clerk could access a taxpayer's account and enter fraudulent information without detection, so long as no paper application was submitted to trigger the front-end screening process. After reviewing this with the Collections Director, we determined that he was aware of this risk and had previously discussed possible solutions with County IS, including creating a screen with fields to track modifications to a taxpayer's record. However, no action was taken to correct this deficiency.

The tax relief programs are a challenge to manage and control due to the legacy tax application currently in use by the County. The County will be implementing a new Tax Administration System (CCI *CollectWare*) within the next 18 to 24 months. The new system will provide audit trails. The Treasurer's Office should continue its participation in the system's development group to insure that controls to detect unauthorized changes to a taxpayer's record are adequately addressed with the current tax application.

In the *COSO's Integrated Framework* report, internal controls are described in terms of their objective and the related control activities. One prescribed objective is to verify the existence or validity of financial transactions to ensure that only valid and authorized transactions are processed. Proper tracking and control of modifications to a system are control activities designed to assure the validity of records and transactions. Currently, not tracking tax-relief clerks' modifications to taxpayer records does not meet this objective. The current lack of access control does not provide adequate internal controls to mitigate the risk that fraudulent information could be entered in a taxpayer's record and go undetected.

***RECOMMENDATION*:**

The Treasurer's Office should continue its multi-year efforts with County IS to implement a series of fields in the taxpayers' records that would track the employee who performed each step in the tax-relief application process. This would allow supervisors to detect unauthorized modifications to taxpayers' records.

ACTION TAKEN:

As an interim, partial solution, the Treasurer recently implemented the capture of notes entered into the tax relief application that creates a database of the note, operator ID, and date and time of entry.

ACTION IN PROCESS:

The Treasurer's Office is taking action to validate that the County's new tax administration system has adequate detective change-control capability to mitigate the risk of undetected change to a taxpayer's record.

3.0 Accounting

Investing Activities

We examined areas related to the Treasurer's capital management and investment responsibilities, as defined by the State Money Management Act, to determine if controls were adequate to protect access, movement, accounting, and reporting of investments managed by the Treasurer. We flowcharted processes to identify control weaknesses and traced investment transactions. Overall, we found adequate controls in place and accurate reporting of pertinent information.

During the course of our audit, we observed that some daily processes were manual, such as the reconciliations of bank accounts, tax postings, and daily tax collection activities. These processes revolved around printing various reports from the bank website, TRGL, and the County's mainframe tax system. Printed reports were used in a number of Treasurer's Office processes, and often reconciled or reviewed by hand.

The printed reports were substantial in volume, many exceeding 50 pages in length. Printing these reports daily represents a sizable requirement for paper use and storage. The reports were also cumbersome, especially when searching for specific information. Our audit tests required a sample of checking-account transactions and we requested electronic copies of bank statements in the form of spreadsheets. The staff accountant stated that only printed copies of the statements were available. He said that the bank did not offer the option of downloading the information in electronic spreadsheets.

We demonstrated to the staff accountant that downloaded transaction data was available from the bank. However, the bank only stores three-month's worth of downloadable detailed transactions online, at any point in time. Daily bank transactions downloaded and stored in electronic format, could greatly reduce the Treasurer's Office storage requirements for paper hard copy documents. In addition, common software applications, such as Microsoft Office Excel (Excel), contain features that can be used to take downloaded information and perform routines on the downloaded data automatically. For instance, daily transaction data could be downloaded from a bank website into Excel, and then the data could be reconciled with account information automatically, without the need for a daily printed copy of transaction data, which is reconciled by hand.

Reconciliations could be performed using electronic data rather than printed reports.

Having electronic copies of documents would have greatly improved our ability to obtain information and saved time in our sampling and testing throughout the audit. Moving towards a more automated and "paperless" office could improve Treasurer's Office operations, and could allow the Treasurer to reduce or reallocate the amount of resources required to manage, work with, and store hard copy documents.

Using modern technology, it is possible to achieve a paperless office, which could offer benefits such as:

- ***Cost-savings*** – through reduced printing and storage
- ***Efficiency*** – through a central online repository that is immediately searchable
- ***Clear audit trails*** – through logged-user access
- ***Improved data availability*** – through online storage for efficient verification, extraction, and analysis
- ***Reduced risk of loss*** – through regular backup of networked data
- ***Improved customer service*** – through efficient access to online documents

We encourage the Treasurer's Office efforts in exploring the concept of a paperless environment.

County Debt Issuance and Management

The Treasurer is a member of the Salt Lake County Debt Review Committee (DRC). County Ordinance §2.97.050, stipulates that the DRC is composed of eight members representing various elected offices and the County Council. According to the mission statement,

> *"The purpose of the Debt Review Committee is to review all debt proposals which anticipate that repayment will occur beyond one fiscal year, and to make recommendations regarding the proposed debt to the County Mayor, and the County Council prior to the debt obligation being incurred."*

It is an objective of the DRC to maintain the County's 'AAA' credit rating from the three major national rating agencies: *Moody's Investors Service, Standard & Poor's, and Fitch Ratings*. In this regard, Salt Lake County holds a unique and prestigious position as one of 22 counties out of 3,033 counties nationwide maintaining their 'AAA' credit rating from all three national rating agencies.

The Treasurer oversees the funding of principal and interest payments for County debt, such County General Obligation (GO) bonds. Payments on County debt obligations are issued bi-annually, with interest-only payments issued at mid-year, followed by both interest and principal payments at year-end.

The GO bond approval and issuance process involves a series of coordinating efforts involving a number of stakeholders, including input from subject-matter experts. These include the County's investment advisor, bond counsel, as well as the national bond-rating agencies. The stakeholder involvement in this process provides due-diligence oversight that significantly mitigates risk.

To identify any possible control weaknesses in these processes, we examined the master bond schedule provided by the Mayor's Fiscal Office, and sampled the four currently issued GO bonds listing the Treasurer's Office as the paying agent. As stated above, the process of issuing GO bonds is deliberative and involves various stakeholders, has multiple review points, and may take as long as 18 months from proposal to issuance. We created a flowchart of this process, which can be reviewed at Appendix E.

In our test work, we reviewed segregation of duties, conflicts of interest, independent review and approval steps, and external reporting. Our audit tests included interviewing the Mayor's fiscal staff, reviewing DRC meeting minutes, and reconciling principal and interest payments. We did not observe any control weaknesses in the process.

We reviewed the Official Statements (OS) issued with the GO bond indenture agreement between the County and the bondholders. The OS included a debt-service schedule for life of the bond. We also examined the process followed by the Treasurer in making debt-service payments. These included the following:

- Prior to payment due date, the bank serving as the "securities depository" issued a transmittal letter to the Treasurer detailing the payments due on bond interest and principal.
- After verifying the transmittal against the OS debt-service schedule, accounting staff set up a wire-transfer to transmit the funds.
- The Deputy Treasurer reviewed and approved the funds for release.
- Debt-service funds were always transferred from the State PTIF account into the County's general account, on the due date without exception.

We traced the timeliness and accuracy of these payments disbursed through the TRGL over the period of the audit. No exceptions were found in the Treasurer's Office records.

Funding County General and Payroll Warrants

Daily general warrants are processed through the Auditor's Office Accounts Payable Division. Authorizations from the Auditor and the Mayor's Office are required before transfer of funds to the warrant clearing accounts. There are two checking accounts set up, one for the electronic funds transfer (EFT), and the other for issuance of manual warrants.

The basic procedures for processing general warrants are as follows:

- The warrant-register listing both manual warrants and EFT amounts, is reviewed and approved independently by the Mayor and Auditor's offices, then forwarded to the Treasurer.

- A journal entry is created and posted to the TRGL by the Senior Accountant.
- The approved warrant-transfer amount is entered into the "Blue Book," (an internal document used to determine the daily cash position of the County) by the Senior Accountant.
- Both the journal and the "Blue Book" entries are reviewed and approved by the Accounting Division Director.
- The previous day's warrant fund transfers, manual and EFT, are verified by the Accounting Division Director to determine the adequacy of the County's current cash position.

ACH transfers of funds are entered into the Wells Fargo Bank Commercial Electronic Office online application by a staff accountant. The transfer is approved for release by one of the following: the Treasurer, the Deputy Treasurer, or the Accounting Division Director. Office policy and system design require a dual authorization of all ACH transfers. To understand and document these procedures, we prepared a flowchart of this process, attached as Appendix F.

Our finding in this area is as follows:

- ***The County's general-warrant checking account, unlike any other warrant-funding account, consistently had a significant excess balance, which created a risk for misappropriation.***

3.1 The County's general-warrant checking account, unlike any other warrant-funding account, consistently had a significant excess balance, which created a risk for misappropriation.

The County Treasurer maintains a reserve above the approved accounts-payable (warrant register) payment balance. The accounting staff members of both the Treasurer's and Auditor's Offices have designated this balance as the "Treasurer's Investment" portion of the general-warrant checking account. This account is an interest bearing checking account from which all manual warrants issued by the County clear.

During the period of our tests, the "Treasurer's Investment" portion of this account ranged between $9 and $25 million, averaging $15.3 million per month. Risk arises from operating an account from which a monthly average of 3,060 warrants cleared. The risk is related to manual warrants having the County's bank account and routing numbers imprinted on them.

Especially for a sophisticated hacker, the opportunity of obtaining unauthorized access, either internally or externally, to this account is made easier by a combination of access to account/routing numbers and significant excess balances in a very active account. Because we are in an era of rampant identity theft and account hacking, maintaining a large

cash balance, never reaching an acceptably cushioned balance with each warrant-funding transfer, presents vulnerability worthy of further review.

To view this in another way, we compared the "Treasurer Investment" balance against the ending general-warrant checking account balance to determine if outstanding warrants were adequately covered. The test showed that the average excess balance (the Ending Account Balance minus the "Treasurer's Investment") was about $3.4 million.

Figure 1 below illustrates this comparison and shows that, exclusive of the "investment" portion, the general-warrant checking account balance was well cushioned to absorb warrant payments.

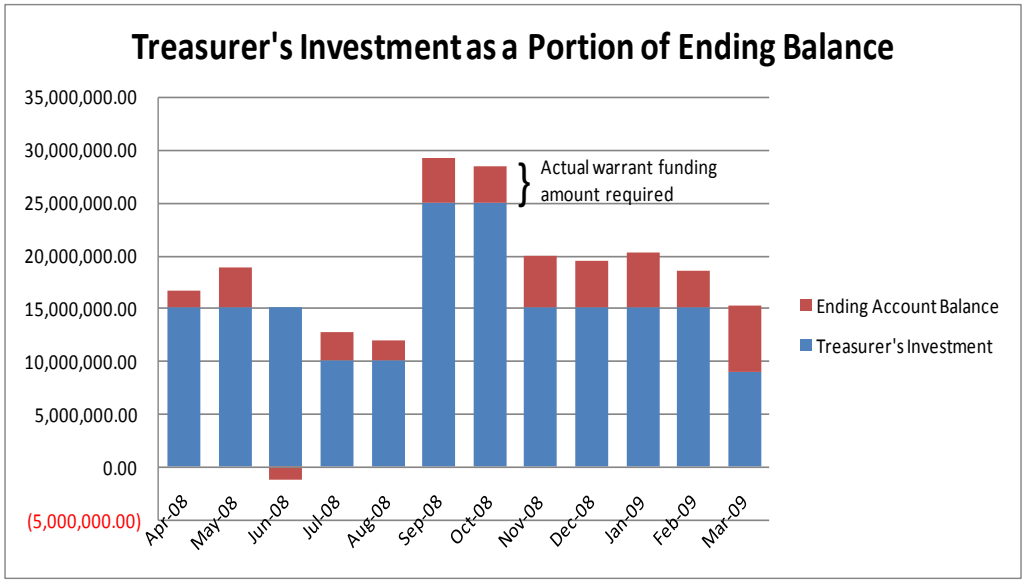


Figure 1. ***Treasurer's Investment amount as a portion of the total ending balance of the general warrant checking account.***

Analysis of warrants cleared demonstrates how broadly the routing and account numbers are distributed. The number of cleared warrants for each month ranged from a low of 2,441 to a high of 5,501 for a year total of 36,716, as shown in Figure 2 on Page 37.

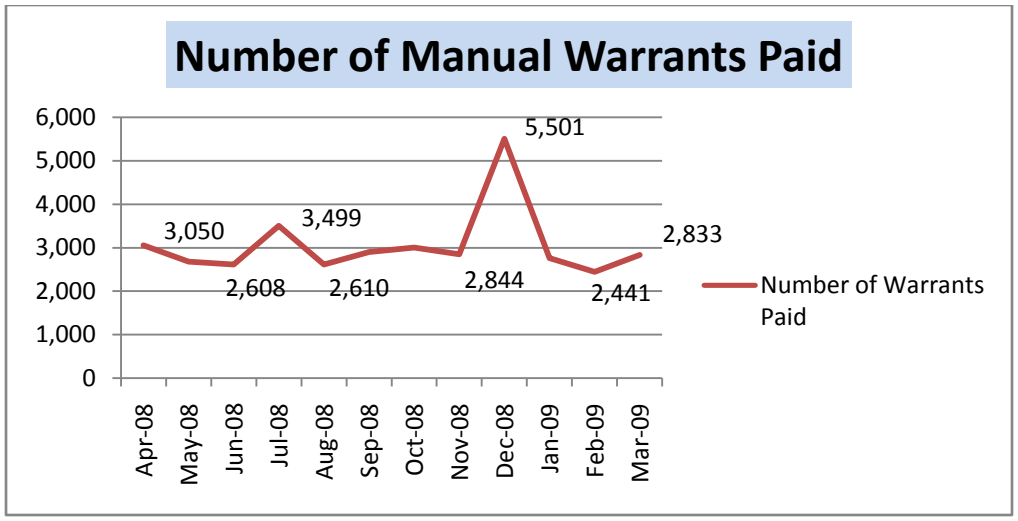


Figure 2. ***Number of manual general warrants cleared from the general warrant checking account per month.***

Widely accepted best practices suggest methods of managing cash disbursements and cash account reconciliations. The most common practice suggests that approved cash disbursements should draw the disbursement account to a zero balance. This control on cash disbursements prevents the account from carrying a balance beyond the payment of approved accounts payable (warrants). This practice reduces the risk for unauthorized payments and facilitates quick identification of fraudulent activity.

The Treasurer Office has always maintained an extra balance or cushion in the warrant checking account designed to address the daily uncertainty in the warrant issuance process. We understand the need to maintain some cushion in the account, especially when this account is not maintained in the County's principal bank account, a situation that does not facilitate the quick movement of money.

The potential for cash transfer delays was exacerbated with events that unfolded after the September 11, 2001 terrorist attacks on the World Trade Center. Funds transfers from secondary bank accounts or outside investment accounts to the primary checking account experienced up to a week's delay, hindering payroll and accounts payable payments. The stability of U.S. financial institutions was questionable and a fear of continued market illiquidity in outside investments prevailed. As a precautionary measure, the County Treasurer transferred County funds out of these external investments and holdings at other banks and into the general-warrant checking account.

After the financial markets stabilized, the practice of keeping a reserve or "Treasurer's Investment" segment in the general-warrant checking account continued. The Deputy Treasurer cited the continued concern over access to liquid investments as a priority over better rates of investment return from outside institutions, especially during poor economic conditions. The economic recession, starting in October 2008,

further renewed and bolstered the Treasurer's emphasis on this priority of maintaining easy access to liquid County funds.

A less risky practice would be to have a separate interest-bearing account. The separate account would provide the liquidity required by the Treasurer, yet would not expose such a large amount of excess County funds to potential theft or misappropriation through account hacking.

***RECOMMENDATIONS*:**

Because there is a demonstrated $3.4 million average monthly float, the Treasurer could fund the general warrant checking account as a zero-balance account.

The Treasurer should consider transferring the "Treasurer's Investment" portion held in the general-warrant checking account into a separate account.

ACTION TAKEN:

In April 2010, the Treasurer's Office transferred $9,000,000, representing the "Treasurer's Investment" portion, out of the general-warrant checking account.

TRANSFERRING FUND # _____ ORGANIZATION # _____ ORGANIZATION NAME _____

SALT LAKE COUNTY PERSONAL PROPERTY TRANSFER/DISPOSAL/INTERNAL SALE FORM PM-2

FIXED ASSET/ PROPERTY ID #	PERSONAL PROPERTY DESCRIPTION	VEHICLE VIN NUMBER/ SERIAL NUMBER	RECV FUND	RECV: ORG:	AUTHORIZED SIGNATURE	TYPE OF TRANSFER	DATE OF TRANSFER	BID/AUCTION OR INTRNL SALE AMNT

FIXED ASSET/DISPOSAL OR TRANSFER CODES

A) TRANSFER TO OTHER ORGANIZATIONS
B) INTERNAL SALE TO/FROM PROPRIETARY FUND
C) TRADE-IN TO VENDOR/NEW EQUIP.PURCHASE (EXPLANATION ATTACHED)
D) CONSIGNED TO SURPLUS FOR TRANSFER/DISPOSAL/SALE
E) UNACCOUNTED FOR/DESTROYED/LOST/STOLEN (COMMISSION LETTER REQUIRED)

INSTRUCTIONS FOR INTERNAL SERVICE/ENTERPRISE FUNDS

1) ITEMS TRANSFERRED TO OR FROM PROPRIETARY FUNDS MUST HAVE AN AGREED UPON PRICE BEFORE THE TRANSFER CAN TAKE PLACE.
2) IF YOUR ORGANIZATION INTENDS TO RESERVE SURPLUS EQUIPMENT FOR THE NEXT AVAILABLE SALE, YOU MUST MAKE STORAGE ARRANGEMENTS WITH THE PROPERTY AGENT IN PURCHASING BEFORE DELIVERY OF ITEMS.

AUTHORIZED SIGNATURE OF TRANSFERRING FUND/ORGANIZATION

_____

AUTHORIZED SIGNATURE OF RECEIVING FUND/ORGANIZATION

_____

SIGNATURE OF SURPLUS PROPERTY AGENT (AS CONSIGNEE OR AGENT)

_____

PM-2'S THAT ARE NOT PROPERLY SIGNED BY BOTH THE TRANSFERRING/RECEIVING ORGN AND/OR PROPERTY AGENT WILL BE RETURNED AND DELIVERY OF SURPLUS ITEMS REFUSED.

TERMS AND CONDITIONS FOR MERCHANT AGREEMENT
(GOVERNMENT ENTITY)

1. Merchant's Acceptance of Cards.

1.1 Exclusivity. You will tender to us Sales Data generated from all your Card transactions via electronic data transmission according to our formats and procedures. You will not use the services of any bank, corporation, entity, or person other than Paymentech for authorization or processing of Visa or MasterCard transactions throughout the term of this Agreement.

1.2 Certain Card Acceptance Policies. Each sale you make involving a Card must be evidenced by a single Sales Data record completed with (i) the transaction date; (ii) a brief description of the goods or services sold, returned, or cancelled; (iii) the price of the goods or services, or amount of any credit or adjustment; (iv) the Cardholder name; (v) your name in a manner recognizable to Cardholders; (vi) your address; (vii) any applicable terms and conditions of the sale; and (viii) any other information that the applicable Association may require. You shall not impose any surcharge or finance charge on the Card transaction or otherwise require the Cardholder to pay any fees payable by you under this Agreement. You shall not set a dollar amount above or below which you refuse to honor otherwise valid Cards. With respect to any transaction for which a Card is not physically presented, such as in any on-line, mail, telephone, or pre-authorized transaction, you must (i) have notified us on your application or otherwise in writing of your intention to conduct such transactions and secured our agreement to accept them and (ii) have reasonable procedures in place to ensure that each Card sale is made to a purchaser who actually is the Cardholder or the authorized user of the Card. Notwithstanding the foregoing, you acknowledge that under the Association Rules, you cannot rebut a Chargeback where the Cardholder disputes making the purchase without an electronic record (for example, "swiping" or "tapping" a Card) or physical imprint of the Card.

1.3 Operating Guide; Association Rules. You agree to comply with the operating guide attached to this Agreement, as amended from time to time ("Operating Guide"), all Association Rules, and with such other procedures as we may from time to time prescribe for the creation or transmission of Sales Data. We may modify and supplement the Operating Guide in order to comply with requirements imposed by the Association Rules. You acknowledge that you have received a copy of the Operating Guide at or prior to your execution of this Agreement, and that you can also view the Operating Guide on-line at the Chase Paymentech Solutions Internet website.

1.4 Requirements for Sales Data. As to each Sales Data you tender to us for processing, you represent and warrant that:

(1) The Sales Data represents payment or refund of payment for the bona fide sale or lease of the goods, services, or both, and the Sales Data is not submitted on behalf of a third party.
(2) The Card transaction represents an obligation of the Cardholder for the amount of the Card transaction.
(3) The Sales Data does not involve any element of credit for payment of a previously dishonored check or for any other purpose except payment for a current transaction and, except in the case of approved installment or pre-payment plans, the goods have been shipped or services actually rendered to the Cardholder.
(4) The Sales Data is free from any alteration not authorized by the Cardholder.
(5) The amount charged for the Card transaction is not subject to any dispute, setoff, or counterclaim.
(6) Neither you nor your employee has advanced any cash to the Cardholder (except as authorized by the Rules) or to yourself or to any of your representatives, agents, or employees in connection with the Card transaction, nor have you accepted payment for effecting credits to a Cardholder's account.
(7) The goods described in each Sales Data submission are your sole property and you are free to sell them.
(8) You have made no representations or agreements for the issuance of refunds except as it states in your return/cancellation policy, which has been previously submitted to us in writing as provided in Section 3.
(9) Any credit transaction submitted to us represents a refund or adjustment to a Card transaction previously submitted.
(10) You have no knowledge or notice of information that would lead you to believe that the enforceability or collectibility of the subject Sales Data is in any manner impaired. The transaction is in compliance with all applicable laws, ordinances, and regulations. You have originated the Sales Data in compliance with this Agreement and the Association Rules.

2. Authorizations.

2.1 Obtaining Authorizations. You are required to obtain authorization/approval codes for all Card transactions by contacting the center designated by Paymentech. You acknowledge that authorization/approval code of a Card transaction indicates only that credit is available for the Card transaction at the time the authorization is given, and it does not constitute a representation from us or from an Association that a particular Card transaction is in fact a valid or undisputed transaction entered into by the actual Cardholder or an authorized user of the Card.

2.2 Lack of Authorization. We reserve the right to refuse to process any Sales Data presented by you (i) if you do not record a proper authorization/approval code, (ii) if we determine that the Sales Data is or will become uncollectible from the Cardholder to which the transaction would otherwise be charged, or (iii) if we determine that the Sales Data was prepared in violation of any provision of this Agreement.

3. Refunds and Adjustments.

3.1 Disclosure of Refund Policy. You are required to maintain a fair policy with regard to the return/cancellation of merchandise or services and adjustment of Card sales. You are required to disclose your return/cancellation policy to us on your application. Your return/cancellation policy must be disclosed to your customers.

3.2 Changes to Policy. Any change in your return/cancellation policy must be submitted in writing to us not less than 14 days prior to the effective date of such change. We reserve the right to refuse to process any Sales Data made subject to a revised return/cancellation of which we have not been notified in advance.

3.3 Procedure for Refunds/Adjustments. If you allow a price adjustment, return of merchandise, or cancellation of services in connection with a Card sale, you will prepare and deliver to us Sales Data reflecting such refund or adjustment within 3 days of receiving the Cardholder's request for such refund/adjustment. The amount of the refund/adjustment cannot exceed the amount shown as the total on the original Sales Data except by the exact amount required to reimburse the Cardholder for postage that the Cardholder paid to return merchandise. You are not allowed to accept cash or any other payment or consideration from a customer in return for preparing a refund to be deposited to the Cardholder's account nor to give cash refunds to a Cardholder in connection with a Card sale, unless required by law.

4. Settlement.

4.1 Submission of Sales Data. You are required to transmit your Sales Data to us no later than the next business day immediately following the day that such Sales Data is originated. You will be solely responsible for all communication expenses required to accomplish the transmission of Sales Data. For debit Card transactions that are credits to a Cardholder's account, you agree to transmit such transactions to us within 24 hours of receiving the

authorization for such transaction. Unless otherwise indicated on Schedule A, you will be solely responsible for all communication expenses required to accept the transmission of Sales Data.

4.2 Merchant's Settlement Account. In order to receive funds from Paymentech, you must maintain a Settlement Account at a bank that is a member of the Automated Clearing House ("ACH") system and the Federal Reserve wire system. You agree not to close your Settlement Account without giving us at least 5 days' prior written notice and substituting another Settlement Account. You are solely liable for all fees, costs, and expenses associated with your Settlement Account and for all overdrafts. You authorize Paymentech to initiate electronic credit and debit entries and adjustments to your bank account at any time without regard to the source of any monies in the Settlement Account. This authority will remain in full force and effect until we notify your bank that all monies due from you under this Agreement have been paid in full. We will not be liable for any of your losses or expenses whatsoever resulting from delays in receipt of funds or errors in Settlement Account entries caused by third parties, including, without limitation, delays or errors by either the Associations or your bank.

4.3 Travel and Entertainment Cards. You cannot submit any T&E Card transaction for processing by Paymentech unless you have a valid agreement in effect with the respective T&E Card company. For the T&E Card transactions designated on Schedule A, upon transmission of such Sales Data by you, we will forward the Sales Data to the appropriate T&E Card company. Except to the extent that we may provide funds settlement services for JCB transactions, payment of the proceeds due you will be governed by whatever agreement you have with that T&E Card company, and we do not bear any responsibility for their performance. If your agreement with a T&E Card company requires the T&E Card company's consent for us to perform the services contemplated by our Agreement, you are responsible for obtaining that consent.

4.4 Transfer of Settlement Funds. For all Card transactions, other than T&E Card transactions, we will process your Sales Data to facilitate the funds transfer between the various Associations and you for Card sales. Promptly after we receive credit for such Sales Data, we will provide provisional credit to the Settlement Account for the proceeds. The proceeds payable to you shall be equal to the amounts received by us in respect of your Sales Data minus the sum of the following: all fees, charges, and discounts set forth in Schedule A, all adjustments and Chargebacks, all equipment charges (if any), all Cardholder refunds, returns, and adjustments, all Reserve Account amounts, and any fees, charges, fines, assessments, penalties, or other liabilities that may be imposed on us or the Member from time to time by the Associations and all related costs and expenses incurred by us. You agree that all such fees, charges, discounts, adjustments, and all other amounts are due and payable by you at the time the related services are rendered to you; that all such Reserve Account amounts are due and payable by you upon our request; and that the related Chargebacks, Cardholder refunds, and adjustments, fees, charges, fines, assessments, penalties, and all other liabilities are due and payable by you when we receive notice thereof from the Associations or otherwise pursuant to Section 4. In the event we do not deduct such amounts from the proceeds payable to you, you agree to pay all such amounts to us. Alternatively, at our option, we may debit the Settlement Account for such amounts. . Also, you agree to reimburse Paymentech, Member, the Associations, affiliates, officers, directors, employees, agents and sponsoring banks from any losses, liabilities, and damages of any and every kind (including, without limitation, our costs, expenses, and reasonable attorneys' fees) arising out of any claim, complaint, or Chargeback (i) made or claimed by a Cardholder with respect to any Sales Data submitted by you, (ii) caused by your noncompliance with this Agreement, the Operating Guide, or the Association Rules, including any breach of a representation or warranty made by you, or (iii) resulting from any voluntary or involuntary bankruptcy or insolvency proceeding by or against you. The obligation provided for in this Section does not apply to any claim or complaint to the extent it is caused by Paymentech's own negligence or willful misconduct.

4.5 Negative Amounts. To the extent Sales Data does not represent sufficient credits or the Settlement Account does not have a sufficient balance to pay amounts due or reasonably anticipated to become due under this Agreement, we may pursue one or more of the following options: (i) demand and receive immediate payment for such amounts; (ii) debit your Settlement Account for the amount of the negative balance; (iii) withhold your settlement payments until all amounts are paid; (iv) delay presentation of your refunds until you make a payment to us of a sufficient amount to cover the negative balance; (v) collect any amount due or which may become due to us from any of your bank accounts without notice to you; and (vi) pursue any remedies we may have at law or in equity. Furthermore, if the amount represented by your Sales Data in any day is negative due to refunds/customer credits being submitted by you in excess of your sales, you are required to provide us with sufficient funds prior to the submission of the Sales Data so as to prevent the occurrence of a negative balance.

4.6 Delinquency/Merchant Fraud. At any time and from time to time we may temporarily suspend or delay payments to you and/or designate an amount of funds that we must maintain in order to protect us against the risk of, among other things, existing, potential, or anticipated Chargebacks and to satisfy your other obligations under this Agreement (such funds being hereinafter referred to as the "Reserve Account"), which may be funded in the same manner as provided for negative balances in sub-section 4.5. The Reserve Account will contain sufficient funds to cover any unbilled processing costs plus our estimated exposure based on reasonable criteria for Chargebacks, returns, unshipped merchandise, and/or unfulfilled services and all additional liabilities anticipated under this Agreement. We may (but are not required to) apply funds in the Reserve Account toward, and may set off any funds that would otherwise be payable to the Merchant against, the satisfaction of any amounts which are or become due from Merchant pursuant to this Agreement. The Reserve Account will not bear interest, and you will have no right or interest in the funds in the Reserve Account. Any funds in the Reserve Account may be commingled with other funds, and need not be maintained in a separate account. Effective upon our establishment of a Reserve Account, you irrevocably grant to us a security interest in any and all funds, together with the proceeds thereof, that may at any time be in our possession and would otherwise be payable to you pursuant to the terms of this Agreement. You agree to execute and deliver to us such instruments and documents (including, without limitation, security agreements and releases) that we may reasonably request (i) to perfect and confirm the security interest and right of setoff set forth in this Agreement; and (ii) in connection with any return of Reserve Account funds.

5. Accounting. We will supply a detailed statement reflecting the activity for your Merchant account(s) by on-line access (or otherwise if we agree). We will not be responsible for any error that you do not bring to our attention within 45 days from date of such statement.

6. Retrieval Requests.

6.1 Records. You are required by the Associations to store original documentation of each Card transaction for at least 6 months from the date of the respective Card transaction, and to retain copies of all such Sales data for at least 18 months from the date of the respective Card transaction. You are not allowed to charge a fee for the creation or storage of such copies. We may, at our discretion, require you to deliver copies of Sales Data to us rather than storing it.

6.2 Response to Retrieval Requests. We will send you any Retrieval Request that we cannot satisfy with the information we have on file concerning any Card transaction. In response, you must provide us in writing by certified or overnight mail or by confirmed fax (or by other means as agreed to by Paymentech) the resolution of your investigation of such Retrieval Request and include legible copies of any documentation required by the Retrieval Request within 7 business days after we send it to you (or such shorter time as the Association Rules may require and of which we notify you). You acknowledge that your failure to fulfill a Retrieval Request in accordance with Association Rules may result in an irreversible Chargeback.

7. Chargebacks.

7.1 Chargeback Reasons. You may receive a Chargeback from a Cardholder or Card issuer for a number of reasons under the Association Rules. The following are some of the most common reasons for Chargebacks:

(1) Your failure to issue a refund to a Cardholder upon the return or non-delivery of goods or services.

(2) An authorization/approval code was required and not obtained.

(3) The Sales Data is prepared incorrectly or fraudulently.

(4) We did not receive your response to a Retrieval Request within 7 business days or any shorter time period required by the Association Rules.

(5) The Cardholder disputes the Card sale or the signature on the sale documentation, or claims that the sale is subject to a set-off, defense, or counterclaim.

(6) The Cardholder refuses to make payment for a Card sale because in the Cardholder's good faith opinion, a claim or complaint has not been resolved, or has been resolved by you in an unsatisfactory manner.

(7) The Card was not actually presented at the time of the sale or you failed to obtain an electronic record or physical imprint of the Card, and the Cardholder denies making the purchase. The Merchant acknowledges that, under these circumstances, the fact that an authorization/approval code was obtained does not mean that a particular Card transaction is a valid or undisputed transaction entered into by the actual Cardholder or an authorized user of the Card.

7.2 Excessive Chargebacks. If we determine that you are receiving an excessive amount of Chargebacks, in addition to our other remedies under this Agreement we may take the following actions: (i) review your internal procedures relating to acceptance of Cards and notify you of new procedures you should adopt in order to avoid future Chargebacks; (ii) notify you of a new rate we will charge you to process your Chargebacks; (iii) collect from you (pursuant to sub-section 4.6) an amount reasonably determined by us to be sufficient to cover anticipated Chargebacks and all related fees, expenses, and fines; or (iv) terminate the Agreement with written notice of termination. You also agree to pay any and all Association fees and fines assessed against you or against Paymentech or Member relating to your violation of the Agreement, the Operating Guide, or the Association Rules with respect to your transactions or with respect to excessive Chargebacks under this Section.

7.3 Claims of Cardholder Customers. You have full liability if any Sales Data for which we have given the Settlement Account provisional credit is the subject of a Chargeback. Subsequently, you are allowed to resubmit applicable Sales Data for a second presentation, but only in accordance with Association Rules. To the extent that we have paid or may be called upon to pay a Chargeback or refund or adjustment for or on the account of a Cardholder and you do not reimburse us as provided in this Agreement, then for the purpose of our obtaining reimbursement of such sums paid or anticipated to be paid, we have all of the rights and remedies of such Cardholder under applicable federal, state, or local laws and you authorize us to assert any and all such claims in our own name for and on behalf of any such Cardholder customer individually or all such Cardholder customers as a class.

8. Advertising. Wherever you accept Cards, you will inform the public of the Cards that you honor. However, you may not indicate that any Association endorses your goods or services.

9. Fees.

9.1 Schedule A. You agree to pay us for our services as set forth in Schedule A in accordance with this Agreement. Unless otherwise expressly stated in Schedule A, such pricing is based on all transactions qualifying under the Association Rules for the lowest Association interchange rates. For Sales Data that does not qualify for the best rate, Association interchange fees provide for a "down-grade," and we will apply a higher rate than the qualifying rate shown on Schedule A. Fees payable under this Agreement that contain a fraction of a cent will be rounded up to the next full cent.

9.2 Price Changes. Notwithstanding anything in this Agreement to the contrary, the prices set forth in Schedule A will at all times be the same as the prices set forth in Contract #PD1896 between the State of Utah and JP Morgan Chase Treasury Services dated on or about June 6, 2005.

10. Termination.

10.1 Term. The initial term of this Agreement shall commence on the earlier of (i) our acceptance hereof (as evidenced by the execution of the Agreement by us) or (ii) 5 days after the Agreement is executed by the Merchant and submitted to Paymentech, and shall continue until either (i) terminated by you by giving at least 30 days' prior written notice to us or (ii) terminated by us by giving notice to you (such termination by us to be effective as of a date set forth in such notice or, if no such date is set forth, to be effective as of the date such notice is received by you).

10.2 Termination for Cause. If our services provided under this Agreement fail to conform to generally accepted standards for such services in the Card processing industry then your sole remedy for such failure shall be that upon notice from you specifying the failure of performance, we will rectify such failure of performance. If we do not rectify our failure of performance within 30 days after receipt of written notification from you, then you may terminate this Agreement upon 30 days' written notice to us. If you terminate the Agreement within the first 3 years following the date of your execution of this Agreement, you agree to pay de-conversion fees of two hundred fifty dollars ($250.00) for each Merchant location that has submitted Sales Data pursuant to this Agreement. Such amount will be funded, to the extent possible, according to the same methods for collecting amounts due under this Agreement. We may terminate this Agreement at any time for any reason upon written notice to you.

10. 3 Account Activity After Termination. Termination does not affect either party's respective rights and obligations under this Agreement as to Sales Data submitted before termination. If you submit Sales Data to us after the date of termination, we may, at our discretion, process such Sales Data in accordance with the terms of this Agreement. Upon notice of any termination of this Agreement, we may estimate the aggregate dollar amount of Chargebacks and other obligations, liabilities, and expenses that we reasonably anticipate subsequent to termination, and you agree to immediately deposit such amount, or we may withhold such amounts from your credits, in order to establish a Reserve Account pursuant to and governed by the terms and conditions of this Agreement.

11. Intentionally Reserved.

12. No Disclosure of Cardholder Information. We will exercise reasonable care to prevent disclosure or use of Card information, other than as permitted under the Association Rules. You will exercise reasonable care to prevent disclosure or use of Card information, other than (i) to your agents and contractors for the purpose of assisting you in completing a Card transaction, (ii) to the applicable Association, or (iii) as specifically required by law. You are prohibited from storing CVV2 or CVC2, magnetic stripe track data, and AVS and PIN data. Each party will store all media containing Card numbers in an area limited to selected personnel on a "need to know" basis only and prior to either party discarding any material containing Cardholder information, the party will destroy it in a manner rendering the Card account numbers unreadable. If at any time either party determines that Card account number information has been compromised, such party will notify the other party immediately and assist in providing notification to the proper parties, as we deem necessary. Merchant information may be shared by us with our affiliates subject to the provisions of this Agreement and Association Rules. You agree to comply with all security standards and guidelines that may be published from time to time by Visa, MasterCard, or any other Association, including, without limitation, the Visa U.S.A. Cardholder Information Security Program ("CISP"), the MasterCard Site Data Protection ("SDP"), and (where applicable) the VISA Payment Application Best Practices ("PABP") (described in more detail in the Operating Guide) (collectively, the "Security Guidelines"). All Service

Providers you use must be recognized by Visa as CISP compliant service providers and payment applications you use must be recognized by VISA as compliant with PABP. You understand that failure to comply with the CISP, SDP or (where applicable) PABP requirements, or other Security Guidelines, or the compromise of any Card account information, may result in assessments, fines, and/or penalties by the Associations, and you agree to reimburse us immediately for any assessment, fine, or penalty imposed on us or the Member due to any such event or your breach of this Section and any related loss, cost or expense incurred by us. You further agree to (i) exercise reasonable due diligence to ensure that all of your Service Providers, agents, business partners, contractors, and subcontractors maintain compliance with the Security Guidelines established by CISP, SDP, and (where applicable) PABP and (ii) provide us upon our request with evaluation of your compliance with Security Guidelines as required by the Associations. If any Association requires an audit of you or any of your Service Providers, agents, business partners, contractors, or subcontractors due to a data security compromise event or suspected event, you agree to cooperate with such audit and agree to pay for all costs and expenses related to such audit, including all of our costs relating to such audit, including attorney's fees.

13. Information About Merchant's Business.

13.1 Additional Financial Information. Merchant agrees to furnish to us upon 5 days' notice such financial statements and information concerning Merchant as we may request.

13.2 Other Information. With prior notice and during your normal business hours, our duly authorized representatives may visit your business premises and may examine only that part of your books and records that pertain to your Sales Data and Card sales. You agree to provide us at least 30 days' prior written notice of your intent to change your product line or services, or your trade name, or the manner in which you accept Cards. If we determine such a change is material to our relationship with you, we may refuse to process Sales Data made subsequent to the change. You agree to provide us with prompt written notice if you are the subject of any voluntary or involuntary bankruptcy or insolvency petition or proceeding. You will also provide us with written notice of any adverse change in financial condition, intent to liquidate, substantially change the basic nature of your business, transfer or sell any substantial part (25% or more in value) of your total assets, or if you or your parent is not a corporation whose shares are listed on a national securities exchange or on the over-the-counter market, change the control or ownership of Merchant or your parent, 30 days prior to such liquidation, change, transfer or sale taking place. You will also notify us of any judgment, writ, warrant of attachment, execution or levy against any substantial part (25% or more in value) of your total assets not later than three days after you obtains knowledge of any such judgment, writ, warrant of attachment, execution or levy.

14. Disclaimer; Limitation of Damages. Subject to Section 5, we will, at our own expense, correct any data in and to the extent that such errors have been caused by us or by malfunctions of our intellectual property or machines. Under no circumstances will Paymentech's financial responsibility for our failure of performance under this Agreement exceed the total fees paid to us under this Agreement (net of Association interchange, assessments, and fines) for the 6 months prior to the time the liability arose. EXCEPT AS OTHERWISE PROVIDED FOR IN THIS AGREEMENT, IN NO EVENT WILL ANY PARTY, ITS RESPECTIVE DIRECTORS, OFFICERS, EMPLOYEES, OR AFFILIATES, BE LIABLE FOR SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR PUNITIVE DAMAGES OR ANY LOSS, THEFT, DISAPPEARANCE, OR DAMAGE TO DATA TRANSMITTED ELECTRONICALLY IN CONNECTION WITH THIS AGREEMENT. WHILE ALL PARTIES ACKNOWLEDGE THAT THIS IS AN AGREEMENT FOR SERVICES TO WHICH THE UNIFORM COMMERCIAL CODE DOES NOT APPLY, PAYMENTECH, MEMBER, AND PAYMENTECH'S SPONSORING BANK HEREBY DISCLAIM ANY AND ALL WARRANTIES WITH RESPECT TO THE SERVICES, PRODUCTS, AND EQUIPMENT PROVIDED HEREUNDER, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR USE FOR A PARTICULAR PURPOSE. **THIS AGREEMENT IS A SERVICE AGREEMENT, AND EXCEPT AS EXPRESSLY PROVIDED IN THIS AGREEMENT, PAYMENTECH AND MEMBER DISCLAIM ALL OTHER REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, MADE TO MERCHANT OR ANY OTHER PERSON, INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES REGARDING QUALITY, SUITABILITY, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR OTHERWISE (REGARDLESS OF ANY COURSE OF DEALING, CUSTOM, OR USAGE OF TRADE) OF ANY SERVICES PROVIDED UNDER THIS AGREEMENT OR ANY GOODS PROVIDED INCIDENTAL TO SUCH SERVICES.**

15. Miscellaneous.

15.1. Intentionally Reserved.

15.2 Application and Credit Check. You represent and warrant that statements made on your Application for this Agreement are true as of the date of your execution of this Agreement. Your signature on this Agreement authorizes us to perform any credit check deemed necessary with respect to Merchant.

15.3 Section Headings. The section headings of this Agreement are for convenience only and do not define, limit, or describe the scope or intent of this Agreement.

15.4 Assignment. We cannot assign this Agreement without your prior written consent, except that we may assign this Agreement to an entity qualified under Association Rules to perform our obligations under this Agreement. You cannot assign or transfer your rights or delegate your responsibilities under this Agreement without our prior written consent.

15.5 Parties. This Agreement binds you and us and our respective heirs, representatives, successors (including those by merger and acquisition), and permitted assigns. You represent and warrant that your execution of and performance under this Agreement (i) in no way breaches, contravenes, violates, or in any manner conflicts with any of your other legal obligations, including, without limitation, your organizational document or any agreement between you and any third party or affiliated entity; (ii) has been duly authorized by all necessary action and does not require any consent or other action by or in respect of any third party; and (iii) that the person signing this Agreement on your behalf is duly authorized to do so. In providing services to you, we will not be acting in the capacity of your agent, partner, or joint venturer, and we are acting as an independent contractor. Each party agrees that any other party may publicly disclose, through press releases or otherwise, the existence of the business relationship that is the subject of this Agreement. Any such disclosure may identify the parties by name but shall not, without the prior written consent of the non-disclosing party, include any of the terms of this Agreement.

15.6 Severability. Should any provision of this Agreement be determined to be invalid or unenforceable under any law, rule, or regulation, including any Association Rule, such determination will not affect the validity or enforceability of any other provision of this Agreement.

15.7 Waivers. No term or condition of this Agreement may be waived except pursuant to a written waiver executed by the party against whom such waiver is sought to be enforced.

15.8 Entire Agreement. The Association Rules, Operating Guide, Application, and all schedules, and attachments to this Agreement are made a part of this Agreement for all purposes. This Agreement represents the entire understanding between Merchant and Paymentech with respect to the matters contained herein. This Agreement shall prevail over the terms of any agreement governing the Settlement Account.

15.9 Notices. Except as otherwise provided in this Agreement, all notices must be given in writing and either hand delivered, faxed, or mailed first class, postage prepaid (and will be deemed to be given when so delivered or mailed), to the addresses set forth below or to such other address as either party may from time to time specify to the other party in writing.

15.10 Governing Law; Waiver of Jury Trial. This Agreement will be governed by and construed in accordance with the laws of the State of Texas without reference to conflict of law provisions. Any action, proceeding, litigation, or mediation relating to or arising from this Agreement must be brought by Paymentech against Merchant in the county and state of Merchant's principal office as indicated below, and by Merchant against Paymentech exclusively in Dallas County, Dallas, Texas. THE PARTIES HEREBY KNOWINGLY, VOLUNTARILY, AND INTENTIONALLY WAIVE ANY RIGHTS EITHER OF THEM MAY HAVE TO A TRIAL BY JURY IN RESPECT OF ANY LITIGATION BASED ON, ARISING OUT OF, OR IN CONNECTION WITH THIS AGREEMENT.**15.11 Force Majeure.** Neither party will be liable for delays in processing or other nonperformance caused by such events as fires, telecommunications or utility or power failures, equipment failures, labor strife, riots, war, nonperformance of our vendors or suppliers, acts of God, or other causes over which the respective party has no reasonable control, except that nothing in this Section 15.11 will affect or excuse your liabilities and obligations for Chargebacks, refunds, or unfulfilled products and services.

16. Survival. The provisions of Sections 4.2, 4.4, 4.5, 4.6, 7, 10.3, 11, 14, 15.10, and 17 shall survive the termination of this Agreement.

17. Definitions.
17.1 "Application" is your statement of your financial condition and the characteristics of account that you have submitted to us on the cover pages of this Agreement and related information, to induce us to enter into this Agreement with you and that has induced us to process your Card transactions under the terms and conditions of this Agreement.
17.2 "Association" is Visa, U.S.A., Inc., MasterCard International, Inc., any debit networks or any other payment method provider.
17.3 "Association Rules" are the bylaws, rules, and regulations, as they exist from time to time, of the Associations.
17.4 "Card" is both (i) the plastic card or other evidence of the account and (ii) the account number, issued to a Cardholder, which you accept from your customers as payment for their purchases from you, which comprise the transactions with respect to which Paymentech agrees to process.**17.5** "Cardholder" is the person to whom the Card is issued and who is entitled to use the Card.
17.6 "Chargeback" is a reversal of a Card sale you previously presented pursuant to Association Rules.
17.7 "Effective Date" means the date on which this Agreement takes effect pursuant to Section 10.1.
17.8 Merchant, "you", and "your" is the Merchant identified in the Application on the cover page of the Agreement.
17.9 Paymentech, "we", "our", and "us" is Paymentech, L.P., a Delaware limited partnership, having its principal office at 1601 Elm Street, Dallas, Texas 75201, by and on behalf of JPMORGAN CHASE BANK, N.A.
17.10 "Retrieval Request" is a request for information by a Cardholder or Card issuer relating to a claim or complaint concerning a Card sale you have made.
17.11 "Sales Data" is the evidence and electronic record of a sale or lease transaction representing payment by use of a Card or of a refund/credit to a Cardholder.
17.12 "Service Provider" is any party that processes, stores, or transmits Cardholder information on your behalf.
17.13 "T&E Card" is a travel and entertainment Card, charge Card, or credit Card issued by American Express or Novus/Discover or such other Card (other than a MasterCard or Visa Card) with respect to which we may agree to process transactions now or in the future.

MERCHANT OPERATING GUIDE
GENERAL RULES APPLICABLE TO ALL TRANSACTIONS

1 Acceptance Of Certain Payment Instruments

In offering Visa and MasterCard payment options to your Customers, you may elect any one of the following options: (i) accept all types of Visa and MasterCard Payment Instruments - including consumer credit and debit/check cards, and commercial credit and debit/check cards; (ii) accept only Visa and MasterCard credit cards and commercial cards (if you choose this option you must accept all consumer credit cards (but not consumer debit/check cards) and all commercial card products, including business debit/check cards; or (iii) accept only Visa and MasterCard consumer debit/check cards (if you choose this option you must accept all consumer debit/check card products (but not business debit/check cards) and will not accept any kind of credit cards). The acceptance options above apply only to U.S. domestic Visa and MasterCard Payment Transactions and, as such, they do not apply to Visa or MasterCard Payment Instruments issued by non-U.S. banks. In other words, if your Customer presents a Visa or MasterCard Payment Instrument issued from a European or Asian bank, for example, you must accept that card just as you would any other card (provided you receive a valid authorization and confirm the identity of the Customer, etc.), regardless of the acceptance option choice you have made and even if you have elected not to accept that type of Payment Instrument from U.S. issuers. If you choose to limit the types of Visa and MasterCard Payment Instruments you accept, the following rules apply to you: (i) you must display appropriate signage to indicate acceptance of the limited acceptance category you have selected (that is, accept only debit/check card products or only credit and commercial products; (ii) if you elect limited acceptance, any Transaction Data submitted into interchange outside of the selected product category will be assessed the standard interchange fee applicable to that card product and may also have additional fees/surcharges assessed; and (iii) additional Visa and MasterCard Rules that may be applicable to you may be viewed on their respective websites.

2 Authorization/Approval Codes

All Payment Transactions and Conveyed Transactions require authorization/approval codes. You must request and receive an authorization/approval code for the total amount of the Transaction. An authorization/approval code indicates (i) the availability of credit on the Payment Instrument at the time of inquiry, and (ii) that the Payment Instrument account number is valid. It is not a promise or a guarantee that you will receive payment for that transaction. It does not warrant that the person presenting the Payment Instrument has the authority to do so.

3 Refunds/Credits

You must disclose your return/refund policy to your Customers. You must complete a credit for the total amount of the refund and identify the merchandise being returned and any shipping and handling charges being returned. You must imprint or record the credit voucher with the same Payment Instrument used to make the original purchase. For retail Payment Transactions and Conveyed Transactions, the credit voucher must be dated and signed by the Customer and the appropriate copy provided to the Customer. Cash refunds should never be issued for Payment Transactions or Conveyed Transactions, unless required by law. If you fail to follow these procedures, you may be unable to rebut a Chargeback from the Customer for failure to issue a refund (even if you actually gave the refund by cash or check). Paperwork is not necessary for an even exchange. For an uneven exchange, complete a credit for the total amount of the merchandise being returned and complete a new Transaction receipt for any new merchandise purchased. You cannot process a credit or refund without having completed a previous purchase Transaction with the same Customer.

4 Processing Of Transaction Data

You must submit Transaction Data (including credit vouchers) to us on or before the next business day after the date of the Transaction. Late submission of Transaction Data may result in higher Payment Brand fees and interchange rates, Chargebacks and other negative consequences. You must not submit Payment Transactions or Conveyed Transactions for payment until the goods are delivered, shipped, or the services are performed (except as otherwise provided in the Merchant Agreement, and only if you have notified us that you are doing so on your application or otherwise in writing). If the Customer disputes being charged for merchandise or services before receiving them, the result will be a Chargeback to you. We may from time to time contact Customers to verify that they have received goods or services for which Transactions have been submitted. You cannot present for processing any Transaction Data that was not originated as a result of an act directly between the Customer and you. You cannot present for processing any Transaction Data you know or should have known to be (i) fraudulent or (ii) not authorized by the Customer. You will be responsible for the actions of your employees while acting in your employ. The collection and payment of all federal, state and local taxes is your responsibility. Taxes collected must be included in the total transaction amount and not collected separately by another form of payment. You must submit one Transaction Data record for all goods and services sold in the same transaction. All available information about the sale, including any handling and shipping charges, must be accurately recorded. You must provide to the Customer a true and completed record of the Transaction.

5 Chargebacks

Chargebacks of Payment Transactions and Conveyed Transactions may occur under a variety of circumstances, as dictated by the Payment Brand Rules, which are subject to modification from time to time. Consequently, the following is only a partial list of circumstances that might give rise to Chargebacks: (i) a Customer account number is incorrect or otherwise invalid; (ii) an authorization/approval code was not received or other required authorization was not obtained; (iii) an authorization/approval code was obtained for the wrong amount or wrong date; (iv) the Customer never received the merchandise/service requested; (v) a Customer's refund/credit was processed as a sale; (vi) the Transaction Data is for the wrong amount; (vii) a Customer was never credited for returned merchandise or a canceled order; (viii) the Payment Instrument was expired, counterfeit, altered, or invalid at time of sale; (ix) a Payment Transaction or Conveyed Transaction was deposited more than once; (x) the Customer did not authorize or consent to the Transaction; (xi) the signature on the Transaction receipt does not match the signature on the Payment Instrument (if required); (xii) the Payment Instrument was not imprinted or its magnetic strip was not electronically recorded (for example, "swiping" or "tapping" a Payment Instrument) through a terminal; (xiii) the Customer asserts any disputes, claim, counterclaim, defense or offset against you; (xiv) the Transaction Data or any material information thereon is illegible, incomplete, inaccurate or unsigned, or is not delivered to us within the required time limits; (xv) the Transaction Data is fraudulent or does not represent a bona fide transaction in the ordinary course of your business, or is subject to any claim of illegality, negligence, dishonesty or offset; and (xvi) you have failed to provide copies of Transaction Data requested by us (retrieval request) within the prescribed time period.

6 Disputing Chargebacks

If you have reason to dispute or respond to a Chargeback, then you must do so by the date provided by us on our report to you. We are not required to investigate, reverse or make any adjustment to any Chargeback when thirty (30) calendar days have elapsed from the date of the Chargeback. All responses to Chargebacks must be in writing, and must contain the following information: (i) date of debit/credit advice; (ii) company case number; (iii) total amount of Chargeback; (iv) date and dollar amount for which the Transaction Data was originally submitted (v) if known, the date and authorization approval code; and (vi) any supporting documentation to substantiate your claim. You should include a dated cover letter detailing reasons for requesting a review of the Chargeback. You should retain a copy of the correspondence and all documentation for your files. You should also retain proof that we received your response.

7 Data Security And Privacy

You agree to post and maintain on all your Web sites both your consumer data privacy policy (which must comply with all Payment Brand Rules, regulations and guidelines) and your method of transaction security. You may not retain or store CVV2/CVC2 data or PIN data subsequent to the authorization. You must comply with all Security Standards published by the Payment Brands and the PCISSC including, but not limited to, Visa's Customer Information Security Program ("CISP), MasterCard's Security Data Program (MSDP) and the Payment Card Industry Data Security Standard (PCIDSS). Pursuant to the Security Standards, you must, among other things: (i) install and maintain a working network firewall to protect data accessible via the Internet; (ii) keep security patches up-to-date; (iii) encrypt stored data and data sent over open networks; (iv) use and update anti-virus software; (v) restrict access to data by employees who are on a "need-to-know" basis; (vi) assign a unique ID to each person with computer access to data; (vii) not use vendor-supplied defaults for system passwords and other security parameters; (viii) track access to data by unique ID; (ix) regularly test security systems and processes; (x) maintain a policy that addresses information security for employees and contractors; (xi) restrict physical access to Customer information; (xii) when outsourcing administration of information assets, networks, or data you must retain legal control of proprietary information and use limited "need-to-know" access to such assets, networks or data; and (xiii) reference the protection of Customer information and compliance with the Security Standards in contracts with other service providers. You must notify Paymentech of any third party vendor with access to Customer information, and you are responsible for ensuring that all third party vendors are compliant with the Security Standards, to the extent applicable. The Security Standards may require that you engage an approved third party vendor to conduct quarterly perimeter scans and/or an on-site security review of your systems in order to be compliant. Visa and MasterCard's individual requirements for such scans or security reviews can be accessed through the Visa and MasterCard websites at www.Visa.com and www.MasterCard.com. The Payment Brand rules provide that Customer information and Transaction Data is owned by the Payment Brand and the Customer. Paymentech also asserts some ownership rights in the Transaction Data to the extent it belongs to the Payment Brand system. You are responsible for securing Customer information. You will not use any Payment Instrument or Customer information other than for the sole purpose of completing the transaction authorized by the Customer for which the information was provided to you, or as specifically allowed by the Payment Brand Rules, or required by law. Paymentech or any Payment Brand may inspect Merchant's premises and computers, and the premises and computers of any company the Merchant has contracted with, for the

purposes of verifying that Customer information is securely stored and processed, and is not used for any purpose other than processing the transactions to which it relates.

8 Certain Merchant Prohibitions

You may not (i) accept Customer payments for previous Visa or Visa Electron charges; (ii) require a Customer to complete a postcard or similar device that includes the Customer's account number, Payment Instrument expiration date, signature, or any other account data in plain view when mailed; (iii) add any tax to a Transaction unless applicable law expressly requires that you be permitted to impose a tax; (iv) request or use a Payment Instrument account number for any purpose other than as payment for its goods or services, except to support Visa's Health Care Eligibility Service or Prepaid Load Network; (v) disburse funds in the form of travelers cheques, if the sole purpose is to allow the Customer to make a cash purchase of goods or services from you; (vi) accept Visa or Visa Electron for the purchase of scrip; or (vii) accept Visa Electron for a manual cash disbursement. You understand and acknowledge that all Visa BIN information provided by us to you is proprietary and confidential information belonging to Visa. You must not disclose Visa BIN Information to any third party without prior written permission from Visa. You understand and acknowledge that Visa may impose conditions on, or permanently prohibit you from participating in the Visa program for any reasons it deems appropriate, including, but not limited to (i) fraudulent activity; (ii) submitting Transaction Data that does not result from an act between you and the Customer (laundering); (iii) entering into this Agreement under a new name with the intent to circumvent provisions of the Rules; (iv) activity that causes us to repeatedly violate the Rules; any other activity that may result in undue economic hardship or damage to the goodwill of the Visa system.

Specialized Rules For Retail Transactions

1 Presentation Of Payment Instruments

You or your employee must examine each Payment Instrument presented to determine that the Payment Instrument presented is valid and has not expired. You must exercise reasonable diligence to determine that the authorized signature on any Payment Instrument) presented corresponds to the Customer's signature on the Transaction Data. You must not honor expired, invalid, altered, counterfeit, or revoked Payment Instruments nor any Payment Instrument presented by any person other than the proper Customer as evidenced by the authorized signature on the Payment Instrument. A Customer may authorize another person to use his or her Payment Instrument for purchases, provided the user's signature appears on the back of the Payment Instrument. The signature on the back must match the one on the Transaction Data. If the Payment Instrument is not signed, in addition to requesting an authorization, you may review positive identification as allowed by local and state law, such as a passport or driver's license, to confirm that the user is the Customer, record the information and require the Customer to sign the signature panel of the Payment Instrument prior to completing the Transaction. You should not complete a Transaction if the Customer does not present his or her Payment Instrument or if you cannot obtain an electronic swipe record or physical imprint of the Payment Instrument (this includes mail, telephone and internet orders). By the submission of any Transaction Data to us, you will be deemed to warrant the identity of the purchaser as the authorized holder of the Payment Instrument, and if the Customer later denies making the purchase, you will not be able to rebut the Chargeback.

2 Completion Of Transactions

You must use a suitable imprinter to legibly imprint Payment Instruments on Transaction Data or, capture the information from the Payment Instrument by electronic data capture. A photocopy of the Payment Instrument is not an acceptable substitute for an imprint. If the account number is manually keyed into the terminal, you must imprint the Payment Instrument. Your name, location, city and state must match the Merchant plate on the imprinter. You must notify us of any changes to the information on the Merchant plate. In addition to having the Customer sign the Transaction receipt, the Transaction date and dollar amounts and other information must be clearly written or printed on the Transaction receipt or captured by an electronic device. A brief description of the goods sold or service rendered must be provided on the Transaction receipt. Authorization/approval code numbers must be clearly recorded in the appropriate place on the Transaction receipt. Never circle or underline any information on the Transaction receipt. Every Transaction Receipt and credit voucher must be imprinted (or printed from electronic draft capture equipment) with the Customer's truncated account number and Merchant name. You will give the Customer a true and completed copy of the Transaction Receipt or appropriate facsimile. If the Customer's copy of the Transaction receipt or credit voucher is printed from electronic draft capture equipment/terminal, it must comply with all applicable Payment Brand Rules and laws. You cannot require Customers to provide any personal information as a condition for honoring Payment Instruments unless otherwise required by the Payment Brand Rules or law. Personal information includes, but is not limited to, a home or business telephone number, a home or business address, a social security number, or a photocopy of a driver's license. You cannot retain or store full magnetic-stripe data, CVV2, CVC2 codes or PIN data after the authorization of a Payment Transaction or Conveyed Transaction, except as required to complete the transmission of such Transaction Data to us.

3 Forgeries/Counterfeit Payment Instruments

You should examine all notices received from us or from a Payment Brand to help you determine whether a Payment Instrument presented is counterfeit. You should attempt to retain the Payment Instrument while making an authorization request and then match any signature on the Payment Instrument with the one on the Transaction receipt. You should compare the account number on the Payment Instrument to the account number printed on the receipt or displayed on the terminal. You should examine each Payment Instrument to see if it looks genuine. You should use reasonable, peaceful efforts to recover any Payment Instrument if you have reasonable grounds to believe such Payment Instrument is counterfeit, fraudulent or stolen. You will be solely responsible for your actions in recovering/retaining Payment Instruments.

4 Travel And Entertainment Services

At your option and as specified in the applicable sections of the Payment Brand Rules, Merchants may participate in one or more specialized travel & entertainment services offered by any of the Payment Brands. Merchants offering travel and entertainment services must institute and comply with the procedures set forth in the Payment Brand Rules.

Specialized Rules for Mail Order, Telephone Order, And Internet Transactions

1 Completion Of Sale

You are responsible for determining that the purchaser is the person whose name appears as the Customer. If an account number is transposed into an invalid or inaccurate account number, the sale will result in a Chargeback. You must be authorized by us to accept Payment Instruments for mail, telephone, internet and pre-authorized orders, and you must have noted such on your application to us. All information that would normally be imprinted from a Payment Instrument must be clearly written in the appropriate areas on the order or Transaction receipt. "Mail Order" or "Phone Order" should be written on the signature line of the Transaction receipt.

2 Recurring Transactions

For recurring transactions, you must obtain a written request from the Customer for the goods and services to be charged to the Customer's account, specifying the frequency of the recurring charge and the duration of time during which such charges may be made. You will not complete any recurring transaction after receiving: (i) a cancellation notice from the Customer (ii) notice from Paymentech or any Payment Brand that the Payment Instrument is not to be honored; or (iii) an authorization/approval code that the Payment Instrument is not to be honored. You must include in your Transaction Data the electronic indicator that the transaction is a recurring transaction.

Specialized Rules for Stored Value Transactions

1 Payment Instruments & Packaging

You may be obligated to purchase Stored Value Payment Transaction Payment Instruments ("Gift Cards") from us or pay us a data transfer fee in lieu thereof. Please check the pricing schedule of your Merchant Agreement to see if these requirements apply to you. If you are obligated to purchase Gift Cards from us or if you elect to do so, we will arrange for the Gift Card production and may, at our option, invoice you therefore, in lieu of electronically debiting your account. Any such invoice will be payable upon receipt. Gift Cards, Packaging and Point-of-purchase marketing materials are available and priced on a per bundle basis, based on current rates. All production and delivery timeframes and costs provided by us are estimates only and we do not guarantee any specific date of delivery or price for Gift Cards produced by third parties. You are responsible for all production costs and delivery charges for Gift Cards. The form and content of all Gift Cards will be subject to our approval.

2 Compliance and Warranties

You are solely responsible for complying with all applicable laws relating to your Gift Card program and you agree to indemnify and hold us harmless from any loss, damage or claim relating to or arising out of any failure to comply with applicable laws in connection therewith. You are solely responsible for monitoring the legal developments applicable to the operation of your Gift Card program and ensuring that your Gift Card program complies fully with such requirements as in effect from time to time. Merchant acknowledges that Paymentech cannot reasonably be expected to monitor and interpret the laws applicable to its merchants, and has no responsibility to monitor or interpret laws applicable to Merchant's business.

3 Fraud

You hereby agree (i) that you are responsible for ensuring that all Gift Cards require activation at the point of sale; (ii) to provide notification in writing to Paymentech of any fraud losses by type by fifteen days following the end of each calendar quarter; (iii) that you will be solely responsible for any and all value adding and fraud losses and expenses relating to or arising from your Gift Card; (iv) to discourage transportation of groups of sequentially numbered Gift Cards; and (v) to deactivate or otherwise remove all value from Gift Cards that have been compromised. You will be responsible for any fraudulent transactions involving your Gift Cards, including, without limitation, the unauthorized activation of Gift Cards, reloading of existing Gift Cards (whether pursuant to a manual telephone order or otherwise) with additional value, or the unauthorized replication of Gift Cards or Gift Card data for fraudulent transactions. Paymentech provides a number of tools and options to help Merchant reduce Merchant's risk of exposure for fraudulent transactions. We urge you to make use of any and all of such tools as we may offer in order to help reduce the risk of such transactions. In particular, we recommend that you utilize only those vendors that have been certified by Paymentech as having appropriate security measures in place to reduce the risk of counterfeit Gift Cards and the loss of sensitive Gift Card information that might result in unauthorized transactions, and we recommend that you promptly and frequently reconcile the transaction reports we provide to you against your own internal transaction records, and to report any unauthorized transactions to your account representative at Paymentech. Because manual Gift Card transactions (i.e. those involving the activation or reloading of Payment Instruments over the telephone in cases where your terminals may be unavailable) pose a higher risk of potential fraud, we urge you to pay special attention to these transactions and reconcile them on an even more frequent basis. In the event that you do not reconcile your transaction reports and promptly report any suspicious activity to us, Paymentech may not be able to assist you in canceling fraudulently activated or reloaded Gift Cards, or in otherwise identifying the source of any fraud.

Global List of PCI DSS Validated Service Providers

As Of 5/1/2009

The companies listed below were validated as being PCI DSS compliant by a QSA as of the "VALIDATION DATE". Service providers are required to revalidate their compliance to Visa on an annual basis, with the next annual Report on Compliance (ROC) due to Visa one year from the "VALIDATION DATE". ROCs that are from 1-60 days late are noted in yellow and ROCs that are from 60-90 days late are noted in red. Entities with ROCs over 90 days past due are removed from this list. Entities are listed in each Visa region where they have been registered by at least one client, including: AP - Asia Pacific, CEMEA - Central Europe / Middle East / Africa, LAC - Latin America / Caribbean, NA - North America - Canada / United States. Visa client's are responsible for and are required to use compliant service providers and to follow up with service providers directly if there are any questions about their compliance status.

List of Compliant Service Providers - All

SERVICE PROVIDER	VALIDATION DATE	SERVICES COVERED BY REVIEW (1)	ASSESSOR	AP	CEMEA	LAC	NA
1ShoppingCart.com	June 30, 2008	Internet Payment Processing	Security Metrics	☐	☐	☐	☑
1st Americard	March 31, 2008	Merchant Payment Services	Trustwave	☐	☐	☐	☑
3C Communications	April 30, 2009	Authorization IPSP (E-commerce) Payment Gateway	Trustwave	☐	☐	☐	☑
3Delta Systems	September 30, 2008	Merchant Payment Services	Fortrex Technologies	☐	☐	☐	☑
A3 IT Solutions	November 30, 2008	Managed Hosting	Trustwave	☐	☐	☐	☑
AAFES	July 31, 2008	Managed Hosting Payment Gateway Payment Processing	IBM Internet Security Systems	☐	☐	☐	☑
ABC Financial	May 31, 2008	Account Billing Services	Trustwave	☐	☐	☐	☑
ABC Virtual Communications, Inc.	November 30, 2008	Payment Processing	SecurityMetrics	☐	☐	☐	☑
Accel Networks	January 31, 2009	Other	Trustwave	☐	☐	☐	☑
Acceptiva	November 30, 2008	Payment Gateway	SecurityMetrics	☐	☐	☐	☑
Accertify	February 28, 2009	Authorization and Settlement	Halock Security Labs	☐	☐	☐	☑
AccountNow	June 30, 2008	Account Management Services	Trustwave	☐	☐	☐	☑
Accounts Receivable Management (ARM)	June 30, 2008	Account Collections	Self-Assessment	☐	☐	☐	☑
Acculynk	February 28, 2009	Authorization	Verizon Business	☐	☐	☐	☑

(1) PCI DSS assessments represent only a "snapshot" of security in place at the time of the review, and do not guarantee that those security controls remain in place after the review is complete. These reviews did not cover proprietary software solutions that may be used or sold by these service providers.

* Current PCI DSS status is under review.

Visa has no duty to clients, merchants, processors or other third parties to obtain or review reports from any party required to submit a report. Visa is not responsible to any party for the timeliness, accuracy or completeness of any report. Inclusion on this list indicates only that the service provider successfully validated PCI DSS compliance, based on the report of an independent Qualified Security Assessor (QSA). Visa does not endorse the service providers or their business processes or practices. Visa has sole discretion to include or exclude entities on this list.

List of Compliant Service Providers - All

SERVICE PROVIDER	VALIDATION DATE	SERVICES COVERED BY REVIEW (1)	ASSESSOR	AP	CEMEA	LAC	NA
CashLINQ Group, LLC	August 31, 2008	Merchant Payment Services	SecurityMetrics	☐	☐	☐	☑
Catalyst Payments	April 30, 2008	Merchant Payment Processing	Trustwave	☐	☐	☐	☑
CBC Companies, Inc	April 30, 2009	Other	Verizon Business, Inc	☐	☐	☐	☑
CBCInnovis, Inc.	April 30, 2009	Other	Verizon	☐	☐	☐	☑
Cboss	November 30, 2008	Payment Processing	SecurityMetrics	☐	☐	☐	☑
CCBill	January 31, 2009	Authorization Clearing & Settlement Internet Payment Processing	Chief Security Officers	☐	☐	☐	☑
CDW Hosting and Managed Services	October 31, 2008	Data-Center Hosting Physical Security	Trustwave	☐	☐	☐	☑
Center Partners	October 31, 2008	Call Center Services	Coalfire	☐	☐	☐	☑
Central Coast Processing	April 30, 2008	Payment Processing	403 Labs	☐	☐	☐	☑
Central States Indemnity	October 31, 2008	Payment Processing	FishNet Security	☐	☐	☐	☑
Centrix Bank – LockBox Service	May 31, 2008	Payment Gateway	SecurityMetrics	☐	☐	☐	☑
Century Bankcard Services	May 31, 2008	Merchant POS Processing	Information Exchange	☐	☐	☐	☑
Certain Software	October 31, 2008	Web-based Reporting	Payment Software Company (PSC)	☐	☐	☐	☑
Certified Payments	September 30, 2008	Payment Processing	Trustwave	☐	☐	☐	☑
CHARGE Anywhere	April 30, 2009	Payment Gateway	Trustwave	☐	☐	☐	☑
Chase Loyalty Solutions	December 31, 2008	Merchant Payment Processing	Trustwave	☐	☐	☐	☑
Chase Paymentech Solutions, LLC.	January 31, 2009	Gift Card Processing Internet Payment Processing Payment Processing	Trustwave	☐	☐	☐	☑
CheckFree PayByPhone	June 30, 2008	Phone Payments	Trustwave	☐	☐	☐	☑
Chip Card Ad Beograd	**February 28, 2008**		Trustwave	☐	☑	☐	☐
ChockStone	September 30, 2008	Gift Card Processing Merchant Payment Processing Stored Value Card Processing	Trustwave	☐	☐	☐	☑
ChoicePay	October 31, 2008	Internet Payment Gateway	K3DES	☐	☐	☐	☑

(1) PCI DSS assessments represent only a "snapshot" of security in place at the time of the review, and do not guarantee that those security controls remain in place after the review is complete. These reviews did not cover proprietary software solutions that may be used or sold by these service providers.

* Current PCI DSS status is under review.

Visa has no duty to clients, merchants, processors or other third parties to obtain or review reports from any party required to submit a report. Visa is not responsible to any party for the timeliness, accuracy or completeness of any report. Inclusion on this list indicates only that the service provider successfully validated PCI DSS compliance, based on the report of an independent Qualified Security Assessor (QSA). Visa does not endorse the service providers or their business processes or practices. Visa has sole discretion to include or exclude entities on this list.

List of Compliant Service Providers - All

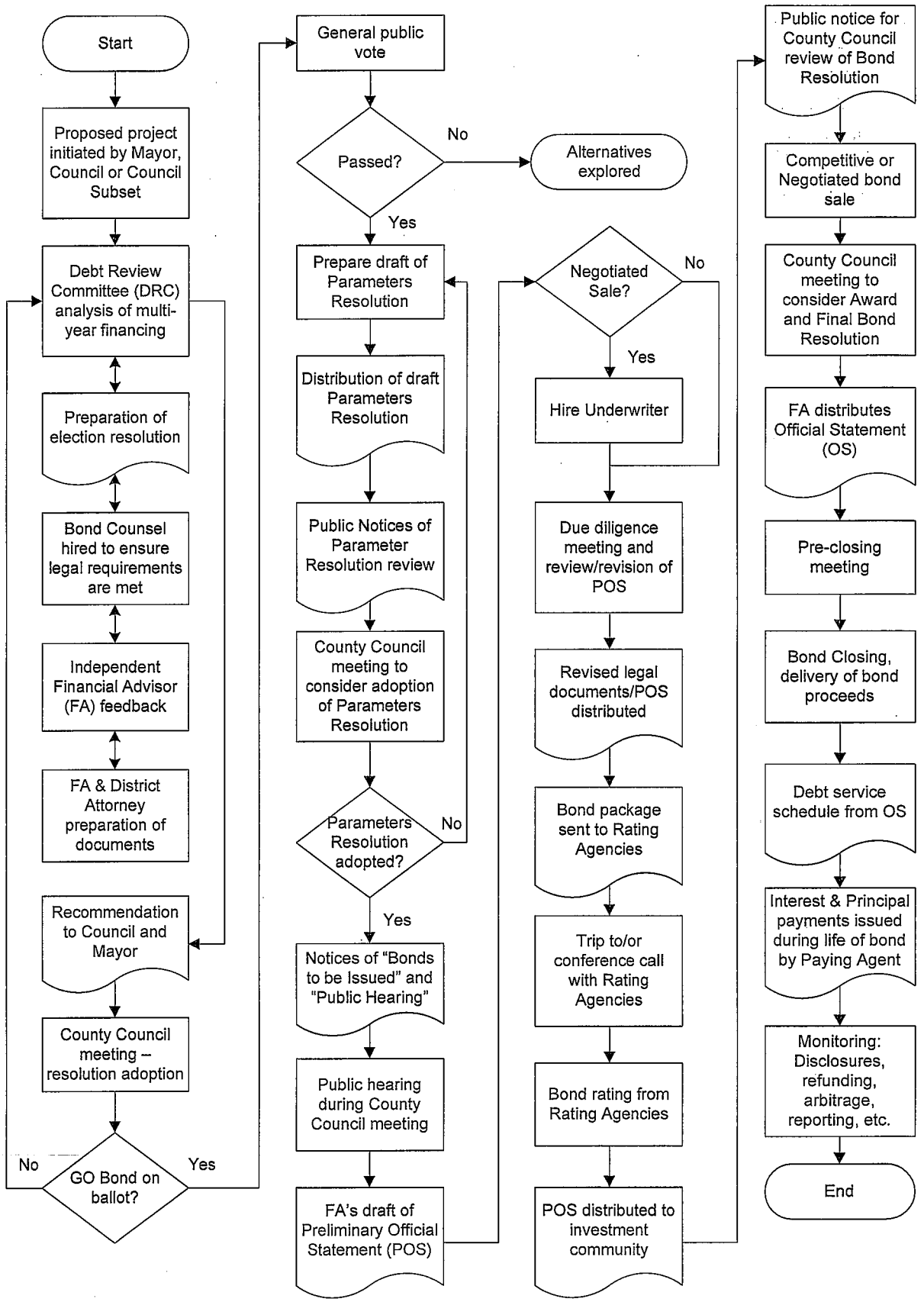
SERVICE PROVIDER	VALIDATION DATE	SERVICES COVERED BY REVIEW (1)	ASSESSOR	AP	CEMEA	LAC	NA
Nelnet Business Solutions, Inc	April 30, 2009	Authorization Payment Gateway	Trustwave	☐	☐	☐	☑
NETBilling	July 31, 2008	Account Billing Services Payment Gateway	SecurityMetrics	☐	☐	☐	☑
NetSpend	December 31, 2008	Authorization and Settlement Issuing Processing Payment Gateway Prepaid Card Processing	Verisign	☐	☐	☐	☑
NetSuite	January 31, 2009		Trustwave	☐	☐	☐	☑
Network Merchants	March 31, 2009	Authorization Clearing & Settlement MOTO Payment Processing Payment Gateway Process Magnetic-Stripe Transactions	Trustwave	☐	☐	☐	☑
Network Solutions	October 31, 2008	Merchant Payment Processing	Payment Software Company (PSC)	☐	☐	☐	☑
New Edge Networks	July 31, 2008	Payment Transmission Services	Trustwave	☐	☐	☐	☑
Newtek Merchant Services	October 31, 2008	Merchant Payment Processing	SecurityMetrics	☐	☐	☐	☑
NEXUS, S.A.	**February 28, 2008**	Issuing Processing	403labs	☐	☐	☑	☐
North American Bancard	October 31, 2008	Payment Processing	Information Exchange	☐	☐	☐	☑
NuComm Marketing Inc.	December 31, 2008	Call Center Services Merchant Payment Processing	Sunera	☐	☐	☐	☑
Nurun	September 30, 2008	Web-based Reporting	Self-Assessment	☐	☐	☐	☑
NYCE Payments Network, LLC	April 30, 2009	Payment Processing	Trustwave	☐	☐	☐	☑
Official Payments Corporation	February 28, 2009	Federal, State, and County Tax Payments Payment Processing	Trustwave	☐	☐	☐	☑
OMS Online, LLC	June 30, 2008	Managed Merchant Hosting Order Fulfillment	SecurityMetrics	☐	☐	☐	☑
OneBridge, Inc.	October 31, 2008	Payment Processing	Crowe Chizek	☐	☐	☐	☑
Open Solutions TotalPlus (Bisys)	April 30, 2009		K3DES	☐	☐	☐	☑

(1) PCI DSS assessments represent only a "snapshot" of security in place at the time of the review, and do not guarantee that those security controls remain in place after the review is complete. These reviews did not cover proprietary software solutions that may be used or sold by these service providers.

* Current PCI DSS status is under review.

Visa has no duty to clients, merchants, processors or other third parties to obtain or review reports from any party required to submit a report. Visa is not responsible to any party for the timeliness, accuracy or completeness of any report. Inclusion on this list indicates only that the service provider successfully validated PCI DSS compliance, based on the report of an independent Qualified Security Assessor (QSA). Visa does not endorse the service providers or their business processes or practices. Visa has sole discretion to include or exclude entities on this list.

Salt Lake County Auditor
Treasurer 2009 Audit
Overview of General Obligation Bond Process



07/30/2009

Treasurer Audit 2009 – Accounts Payable Warrant Flowchart