City of Riverside
Administrative Manual

City of Arts & Innovation

Effective Date: 01/2009
Latest Revision Date: 02/2016
Next Review Date: 07/2018
Policy Owner(s): Finance Department

Approved:

John A. Russo
City Manager

Department

City Manager

SUBJECT:

Credit Card Acceptance Policy

PURPOSE:

Policy Statement and Scope

This policy establishes standards for the acceptance and processing of credit card payments in City departments and maintaining the security of confidential credit card data. The federal Fair and Accurate Credit Transactions (FACT) Act of 2003 requires creditors (defined in the Act to include municipally-owned public utility companies or other public entities that extend credit) to implement reasonable policies and procedures for detecting, preventing and mitigating identity theft. This policy will supplement the City's Identity Theft Prevention Program required by the FACT Act.

Compliance with this policy will:

- Provide reasonable assurance that all credit card transactions are properly authorized, settled timely, and accurately and completely recorded;
- Monitor for errors, both unintentional and intentional, including fraud; and
- Protect the security, confidentiality and integrity of cardholder information.

This policy is further intended to ensure compliance with Payment Card Industry (PCI) Standards, as required by Visa, Mastercard, American Express and Discover. Failure to comply with PCI standards may result in fines and/or revocation of credit card acceptance. Additionally, the City will review EMV (Europay, Mastercard, Visa) fraud liability criteria as it pertains to each City Department. Implementation of EMV ready point-of-sale devices will occur as required by each payment application provider or merchant processor.

POLICY:

Authorized Departments

As of the date of this policy, the following departments are authorized to accept credit card transactions:

- Museum
- General Services (Fleet)
- Community and Economic Development
- Finance
- Fire
- Library
- Parks, Rec. & Community Svc.
- Police
- Public Utilities
- Public Works

Departments anticipating acceptance of credit card payments, whether by Point-of-Sale or electronically driven, are required to obtain Finance Department approval in order to apply for and obtain a Merchant

Account. Additionally, departments must comply with credit card provider regulations, including the acceptance of credit cards for all transaction types and dollar amounts.

Transaction Control Requirements

The City accepts Visa, Mastercard, American Express, Discover, Voyager, and WEX credit cards as a form of payment of amounts due to the City. Debit cards with Visa or MasterCard logos are also accepted and processed as credit cards. The City currently accepts payments through point-of-sale, telephone, internet and mail transactions. Each transaction type requires a unique set of processes to ensure the accurate processing and recording of transactions and guard against erroneous or fraudulent transactions.

It is the policy of the City that usernames and passwords are not shared. City employees processing credit card payments, whether by point-of-sale or through a virtual terminal, must have and use individual logins.

Point of Sale Transactions

1. Credit card machines and manual imprinters are to be secured and inaccessible to the public. However, a customer's credit card should be visible to the customer at all times during the transaction.
2. Prior to processing the credit card, compare the name on the credit card to the cardholder's photo identification. If the names do not match, the credit card must not be accepted for payment.
3. Ensure that the amount charged to the card matches the transaction amount. No refunds or credits may be issued in conjunction with the payment.
4. A signature must be obtained on the credit card payment receipt.
5. If the credit card's chip or magnetic strip cannot be read, the card number should be keyed into the credit card terminal. To reduce the risk of access to confidential credit card data, manual imprints of the card should not be made.
6. When an EMV chip card is presented for payment:
    a. The card must remain in the terminal during the entire transaction to obtain authorization.
    b. If a pin is required for authorization and the cardholder does not know it, the cardholder must present another form of payment.
    c. A transaction authorized by pin does not require a signature for authorization.
7. If the authorization network (via the credit card machine or the Address Verification Service) sends a "decline" or "no match" response, the credit card must not be accepted.
8. In all circumstances of declined or unaccepted transactions, return the credit card to the customer and offer to accept another method of payment. Customers disputing the decline or non-acceptance of the credit card should be referred to their credit card company.

Internet Transactions

1. The website must include fraud prevention measures such as Address Verification Services, Card Certification Value, Card Validation Code, Card Number Encryption, or other tools available through the bank or merchant service provider.
2. Any website dedicated to utility payment processing must prohibit payments from a third-party, as defined in this policy.

Telephone and Mail Transactions

1. Key the credit card data including the cardholder name, card number, expiration date, street number and zip code into the credit card terminal. Failure to key in the address information results in higher credit card fees and increases the risk of fraud.
2. Ensure that the transaction documentation (e.g., remittance advice) contains the customer number, invoice number or other identifier. Do not accept credit card payments from a third-party, as defined in this policy.

Virtual Terminal and Payment Application Access

User access should be defined by user role and function within a department for point-of-sale, internet, telephone, and mail credit card payment processing. Each user should be assigned a unique user ID and password.

Third-Party Transactions

The following conditions qualify as third-party transactions:

1. The name on the credit card does not match the identification of the individual presenting it.
2. For card-not-present transactions, the name on the credit card billing information does not agree with the City of Riverside account name(s).

Third-party Payment Processors

No department will initiate credit card acceptance with a bank, merchant service provider or as a tie-in to third-party software without Finance Department involvement and approval. Any computer system or internet-based payment processing will also require Information Technology review and approval to ensure the third party has adequate safeguards of confidential data in place, such as encrypted data transmission of card information.

The City currently contracts with third-party payment processers to accept credit card payments on behalf of the City. The applicable departments will work with the provider to ensure that a complete and accurate recording of transactions, fees and deposit of monies takes place in a timely manner. All third-party processors are expected to comply with PCI standards as well as EMV standards, where applicable.

Settlement and Deposit of Credit Card Payments

- The daily receipt totals from point-of-sale credit card machines must be printed and used to settle transactions at the end of each business day.
- The transaction history report from each credit card machine must be reconciled to the total credit card receipts.
- The settlement batch, transaction history and reconciliation reports and supporting documentation must be remitted to the Treasury division on the following business day. Any items held overnight in the department must be secured to prevent against the theft of confidential customer data.
- All credit card receipts and supporting documentation that are routed through interoffice mail must be secured in a locked currency bag.
- Deposits are generally credited to the bank within 3 business days, depending upon the credit card type.

Refund of Credit Card Payments

- Refunds must be tied to the original transaction and are limited to the credit card used in that

transaction. If the credit card used in the original transaction has been closed for any reason, the cardholder must initiate the refund process through his/her bank.

- Lead or Supervisor approval must be obtained in order to initiate and complete a refund. The person authorizing a refund must complete and sign a *Request for Credit Card Void/Refund* form and is responsible to ensure that the refund is properly executed and appropriately documented.

- Refunds must be reconciled with the settlement batch and remitted to the Treasury division with all supporting documentation.

Merchant Fees and Other Credit Card Charges

Merchant fees for all point-of-sale transactions are identified on the City's bank statement by merchant account. Departments will be charged their proportional share of merchant fees.

No City Department will charge credit card service or convenience fees unless authorized by City Council.

Credit Card Chargebacks and Disputes

1. Other credit card charges, such as chargebacks and disputed items are related to a specific transaction and will be referred to the appropriate department for follow-up. Departments will work with the Treasury Division to conduct preliminary research and provide supporting documentation to determine if a claim is valid.
2. A fee may be charged to the customer when a chargeback results in the reversal of a payment due.
3. City departments that do not have an established debt collection agency or collection policy may refer to City Finance/Collections to recover such payments when it is established that the cardholder is obligated to re-pay for service received or fees owed.

Safeguarding of Confidential Data

- Credit card records, including but not limited to, receipts, imprints, credit card numbers, expiration date, card type, bank information, etc. are exempt from public disclosure and shall not be disclosed by the City unless required via Court subpoena or in writing by the City Attorney.
- Any credit card documents not remitted to Treasury before the close of the business day must be secured to prevent against the theft of confidential customer data.
- If processing of credit card data is provided by a third party on the City's behalf, the service provider must be PCI compliant.
- Full credit card numbers must not be recorded, maintained or viewable in any computer systems.
- To the extent required by law, the City will notify credit card customers of any breach of security which has placed their confidential credit card information at risk.

Payment Card Industry (PCI) Compliance

The City will annually review and update PCI Self-Assessment Questionnaire (SAQ) B-IP and Attestation of Compliance applicable to Validation Type 3 merchants. Merchants in Validation Type 3 process credit card transactions in a variety of manners, including stand-alone and dial-out terminals, and do not store electronic cardholder data. In accordance with PCI standards, quarterly vulnerability scans will be conducted by a PCI SSC approved scanning vendor.

The City will confirm that third-party processors accepting credit card payments on behalf of the City also complete the PCI SAQ applicable to their merchant validation type.

Europay, MasterCard, Visa (EMV) Compliance

The City will review EMV fraud liability protocols regarding non-compliance. If it is deemed necessary, the City will support EMV chip processing by obtaining EMV ready point-of-sale devices at all point-of-sale locations accepting credit card payments. Additionally, the City will ensure that all card reading devices, payment gateways, and payment processors have the appropriate level of EMV certification.

PROCEDURE:

Responsibility	Action
City Department	Follow City policy and procedures established for the processing and settlement of credit card payments.
	Provide adequate training of staff members to ensure compliance with the credit card policy and understanding of the related procedures and internal controls.
	Ensure that all credit card data is adequately safeguarded.
	Utilize locked currency bags when transporting credit card documentation via interoffice mail, and limit access to the currency bag keys to specific, authorized personnel.
	Perform reconciliation of payments to ensure accurate recording of transactions and deposits.
	Perform settlement procedures and remit required data to Treasury in a timely manner.
	Follow up immediately on chargebacks (disputed, returned or rejected items) by conducting preliminary research to determine if a claim is valid.
	Ensure the recovery of monies owed or withdraw or deny services as required in response to credit card chargebacks and disputes.
	Report suspicious activity including possible fraud or theft to the Internal Audit division in a timely manner.
Finance – Treasury	Treasury will follow City procedures relating to bank statement review, credit card deposit verification and review of department data and recording of receipts.
	Forward credit card chargebacks and disputes to the appropriate City Department; ensure that the process is complete and that all relevant documents are forwarded to the bank. Additionally, ensure that bank charges resulting from chargebacks or disputes have a corresponding charge to internal accounts within the appropriate department.
	Record a monthly allocation of merchant fees to each department based upon the department's proportional share of credit card receipts.
	Ensure that all credit card data is adequately safeguarded.
	Report suspicious activity including possible fraud or theft to the Internal Audit division in a timely manner.

PROCEDURE:

Responsibility	Action
Finance Administration	Ensure that City Departments acquire and implement the use of EMV ready devices at all point-of-sale locations where it is deemed necessary.
	Annually review and update the PCI Self-Assessment Questionnaire and Attestation of Compliance.
	Ensure that third-party processors accepting credit card payments on behalf of the City complete the PCI SAQ applicable to their merchant validation type.
	Forward quarterly scan reports to the Bank.
	Approve requests from City Departments for credit card merchant accounts, point-of-sale credit card systems, and payment integration software and services.
	Periodically review and monitor merchant servicing agreements, rates, and fees.
Information Technology	Ensure adequate safeguarding of customer data.
	Ensure the adequacy of the control systems of electronic data of third-party vendors.
	In cooperation with Finance Administration, annually review and update applicable portions of the PCI Self-Assessment Questionnaire and Attestation of Compliance.
	Coordinate quarterly vulnerability scans conducted by a PCI SSC Approved scanning vendor. Address and correct deficiencies identified during the scans and forward the vendor's quarterly scan reports to Finance Administration.
	In cooperation with Finance Administration, implement approved payment integration software. Ensure that system passwords are secure and access is limited to required staff.

Attachment: Request for Credit Card Void or Refund

Distribution: Regular

Request for Credit Card Void/Refund

Void—Occurs same day, before settlement
Refund—Occurs after settlement

Today's Date: _____ Batch Date: _____ Batch #: _____ Transaction #: _____

Charged Amount $_____ Refunded Amount $_____

Account or Document #: _____ Last Four Digits Card #: _____

Reason for Void/Refund: _____

Requested by: _____ Requestor's Initials: _____
Print Name of Representative

Approved by: _____ Approver's Signature: _____
Print Name of Lead, Supervisor, or Manager

Payment Reversed by: _____

MUST include the following documents with settlement report:

- Original credit card receipt (if any)
- All other supporting documentation