

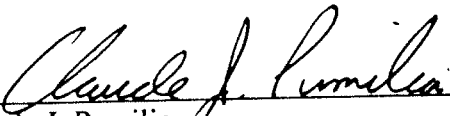
RULES AND REGULATIONS  
CITY AND COUNTY OF DENVER  
MANAGER OF FINANCE

RULES AND REGULATIONS FOR CREDIT CARD PROCESSING AND DATA  
SECURITY REQUIREMENTS

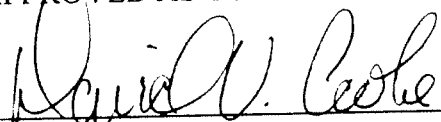
Notice Published  
October 24, 2008  
in  
*The Daily Journal*

Public Hearing Held  
November 13, 2008

APPROVED AND ADOPTED:

  
\_\_\_\_\_  
Claude J. Pumilia  
Manager of Finance, City and County of Denver

APPROVED AS TO FORM:

  
\_\_\_\_\_  
David V. Cooke  
Assistant City Attorney, City and County of Denver

4.15.2009  
\_\_\_\_\_  
Effective Date

Adopted and published pursuant to Article II, Part 5, Section 4 of the Charter of the City and County of Denver and Section 20.36 *et seq.* of the Denver Revised Municipal Code.

Three copies of these rules and regulations are filed – one with the City Clerk, one with the City Attorney's Office, and one with the Office of the Manager of Finance.

**CREDIT CARD PROCESSING AND DATA SECURITY REQUIREMENTS**

**1.00 GENERAL PROVISIONS**

**1.01 PURPOSE**

The purpose of this Rule and Regulation is to set forth the City's policy and requirements for accepting and processing credit cards and for securing any data associated with credit card processing.

**1.02 AUTHORITY**

City Charter, Section 2.5.4  
Revised Municipal Code, Section 20.36  
Visa, MasterCard Operating Guidelines  
Payment Card Industry (PCI) Data Security Standard

**1.03 DEFINITIONS**

- .01 Credit Cards: Only credit cards approved by the Manager of Finance for each agency may be accepted. VISA and MasterCard are approved for all agencies to accept. Upon approval by the Manager of Finance, the agency may accept AMEX, Discover, or credit cards from other providers. All credit card receipts are governed by this Rule and Regulation including in person, by telephone, telefax, mail or by Internet.
- .02 City Agencies: All City departments, agencies, boards, commissions, and offices, along with any City contractors, agents, or concessionaires required to deposit receipts with the Department of Finance.
- .03 Manager of Finance: Shall mean the Manager of Finance of the City or the successor official ("MOF").
- .04 Track 1 Data: contains the cardholder's name as well as account number and other discretionary data.
- .05 Track 2 Data: contains the cardholder's account, encrypted PIN, CVV2, plus other discretionary data.

**1.04 POLICY**

The establishment of control measures for credit card data security is required by the Payment Card Industry (PCI). The City's ability to receive charge card payments is predicated on its compliance with the Cardholder Association's Payment Card Industry Data Security Standards (PCI DSS). Periodic reviews of safeguarding and storage of cardholder information by individual agencies may be conducted by the MOF. City Agencies not complying with approved safeguarding, storage and processing procedures may lose the privilege to accept credit cards.

1.05 APPLICABILITY & RESPONSIBILITY

- .01 This Rule and Regulation is applicable to all City agencies that are required to deposit receipts with the Department of Finance.

2.0 REQUIREMENTS

2.01 THE MANAGER OF FINANCE WILL PERFORM THE FOLLOWING FUNCTIONS:

- .01 Will be a signatory party and hold all contracts for credit card processing unless the MOF determines to delegate this responsibility in writing to an agency.
- .02 Will determine which agencies can accept credit cards and which credit cards the agency can accept.
- .03 Will determine the type of credit card settlement for each agency: real-time authorization and/or settlement, batch authorization and/or settlement, and/or over the counter internet settlement.
- .04 Will designate approved equipment to be purchased and used by the agencies to process credit cards (See Manager of Finance Rule and Regulation titled "ADMINISTRATIVE PROCESSING FEES, NEW EQUIPMENT AND SOFTWARE REQUIREMENTS, AND IMPLEMENTATION QUESTIONNAIRE PROCEDURES FOR ALTERNATIVE FORMS OF PAYMENT" for further details).

2.02 CITY AGENCIES AUTHORIZED TO ACCEPT CREDIT CARDS WILL HAVE AND PERFORM THE FOLLOWING DUTIES:

- .01 Ensuring that the retention of services of any 3<sup>rd</sup> party vendor who provides credit card processing and/or settlement are established through a formal City contract, monitoring contract compliance, and ensuring that the 3<sup>rd</sup> party complies with this Rule and Regulation.
- .02 Establishing departmental procedures for safeguarding cardholder information.
- .03 Performing an annual security self-assessment and report the results to the MOF to ensure compliance with this policy and associated procedures.
- .04 Complying with all applicable provisions of the PCI DSS.

2.03 DATA STORAGE COMPLIANCE

- .01 Electronic – no Track 1 Data beyond 18 months activity will be stored or retained electronically. Any such information will be truncated and encrypted. No Track 2 Data will be retained or stored at any time.
- .02 Hard Copy – no Track 1 Data beyond 18 months activity will be stored or retained by hard copy beyond 18 months. Any such information must be truncated and safeguarded. No Track 2 Data will be retained or stored at any time.

- .03 Internet - no Track 1 Data beyond 18 months activity will be stored or retained electronically. Any such information will be truncated and encrypted. No Track 2 Data will be retained or stored at any time.
- .04 When credit card imprinters must be used due to a failure of electronic processing, the manual form must be retained only until the transaction is entered into the system for processing and verification of processing has been completed.. The account number must then be manually truncated displaying only the first five (5) digits and last four (4) digits. The imprint must be secured under lock and key for no longer than 18 months after which it will be destroyed.

2.04 CARDHOLDER INFORMATION SECURITY PROGRAM (CISP)

- .01 The Self-Assessment Questionnaire (Exhibit 1) must be completed annually by each agency that accepts credit cards and must be provided to the MOF. The MOF may require agencies to provide the completed questionnaire to the MOF more frequently.
- .02 Any agency utilizing a 3<sup>rd</sup> party vendor for credit card processing and/or settlement may undergo a forensic and/or physical assessment investigation by a MOF-contracted provider, whose professional services are retained by way of formal City contract, at the discretion of the MOF. This process may include a security assessment and infrastructure scan. The results of this assessment investigation will be maintained by the MOF
- .03 Any agency utilizing Internet settlement for credit card processing and/or settlement may undergo a forensic and/or physical audit investigation by the MOF contracted provider at the discretion of the MOF. This process may include a security audit and infrastructure scan. The results of this audit investigation will be maintained by the MOF.
- .04 The MOF may forward the results of any charge card data security assessment investigation(s).

2.05 FEES

- .01 The MOF will determine payment of credit card processing fees and how they are accounted for in all agencies unless the MOF designates this function to an agency in writing.
- .02 Agencies who are found to be out of compliance may be held responsible by the MOF for payment of the assessment investigations resulting from the non-compliance.

2.06 CHARGEBACKS AND RETRIEVALS

- .01 Each agency will be responsible to receive notice of chargebacks and retrieval requests for each of their merchant IDs.
- .02 Each agency shall research and provide all necessary data to counter a dispute if the agency determines the dispute is in error within the chargeback notification's timeframe.

- .03 Each agency will work with customers and credit card processing providers to settle claims accurately and timely.
- .04 Each agency will account for any chargebacks that are successful in accordance with the practices established by the MOF.
- .05 If a chargeback or retrieval has been issued, each agency must respond to the credit card processing provider to reserve the City's rights under the current contract.

6-30-08