OREGON ACCOUNTING MANUAL

Subject:	Accounting and Financial Reporting	Number:	10.35.00.PR
Division:	State Controller's Division	Effective date:	April 17, 2008
Chapter:	**Internal Control**		
Part:	**Credit Card Acceptance for Payment**		
Section:			
Approved:	John Radford, State Controller	Signature on file at SCD	

Purpose and Scope

.101 This procedure describes internal controls and safeguards that must be implemented to:

a. Provide reasonable assurance that all credit card transactions are properly authorized, timely settled, and accurately and completely recorded;

b. Reduce the risk of unauthorized access and to monitor for errors, both unintentional and intentional errors, including fraud;

c. Protect the security, confidentiality and integrity of cardholder information; and

d. Comply with notification requirements in the event of a security breach.

.102 The requirements set forth in this procedure apply to all state agencies that process credit card transactions. Each agency that accepts payments by credit cards has a responsibility to understand the unique issues of operating its e-commerce program and to create internal policies and procedures to address those issues. Agencies are encouraged to contact the Office of the State Treasurer (OST) and the State Controller's Division (SCD) to learn more about the various tools and controls available to reduce exposure to e-commerce risks and minimize the associated losses. OST can also advise agencies on ways to process credit card transactions that will increase efficiency and reduce transaction fees.

.103 None of the controls described below relieves agencies of their responsibility to comply with policies published by OST, the US Bank Merchant Terms of Service (MTOS) or Discover Business Services Merchant Operating Regulations (MOR). Agencies must adhere to OST policies and the MTOS/MOR. When credit card fraud is suspected, for example, agencies must refer to the MTOS/MOR guidelines.

Point of Sale (POS) Transactions – Control Requirements

.104 Agencies that accept and process credit cards in payment of products, services, licenses, or other fees in face-to-face transactions conducted over the counter must incorporate the following control procedures into their operations.

a. Before swiping the customer's credit card through the POS terminal, verify that the card expiration date has not passed. **Expired credit cards must not be accepted for payment.**

b. Ensure that the dollar amount charged to the card is fixed by the transaction. **No cash refund or credit may be issued in conjunction with the purchase transaction.**

c. If the authorization network approves the transaction, ask the customer to sign the sales receipt and then compare the customer's signature with the signature on the back panel of the credit card. **Unsigned cards must not be accepted.**

d. Compare the name and account number on the credit card with the name and last four digits of the account number on the printed receipt. **Refer to the MTOS/MOR if the name or digits do not match.**

   NOTE: The MTOS/MOR requirement that all POS devices must suppress all but the last four digits of the credit card account number and the entire expiration date on the cardholder's copy of the transaction receipt is consistent with Oregon law. The Oregon Identity Theft Prevention Act (Oregon Laws 2007, Chapter 759) states that data shall be redacted so that no more than the last four digits of a customer's credit or debit card number are accessible.

e. If the credit card's magnetic stripe cannot be read, and the cardholder's information is key-entered, agencies must:

   - Request Address Verification Services (AVS).
   - Make a physical imprint of the card using a manual imprinter.
   - Obtain the cardholder's signature on the imprinted transaction receipt and compare it to the signature on the back panel of the card. **Unsigned cards must not be accepted.**
   - Black-out all but the last four digits of the credit card number on the cardholder's copy of the receipt.

f. To complete the transaction, information necessary for the delivery of purchased goods or services may be requested and recorded as long as the information is provided voluntarily by the credit cardholder (**ORS 646A.214**).

.105 If a "declined" or "no match" response is received from the authorization network, the credit card cannot be accepted. Agencies shall offer to process a different, valid credit card or another acceptable form of payment, such as a personal check or cash.

Telephone and Mail Order Transactions – Control Requirements

.106 Agencies that accept and process credit cards in payment of products, services, licenses, or other fees in transactions that are conducted by telephone or mail order must incorporate the following controls into their operations.

a. Request Address Verification Services (AVS).

b. Ensure that the transaction documentation includes the agency's order number (e.g., invoice number, license number or similar identifier) and the agency's customer service number.

Internet Transactions – Control Requirements

.107 Agencies that accept and process credit cards in payment of products, services, licenses, or other fees in transactions that are conducted over the Internet must incorporate these additional controls into their operations.

a. If products and/or services have a fixed fee, the system must populate the amount field based on the customer's selection.

b. The Internet website must incorporate fraud prevention measures, such as Address Verification Services (AVS), Card Verification Value (CVV2), Card Validation Code (CVC2), or other fraud prevention tools available through the issuing bank. Refer to the MTOS/MOR for further information.

Fulfillment and Revenue Recognition

.108 Unless the agency and merchant bank have agreed otherwise and such agreement is in writing, any agency accepting payment by credit card must place a "hold" on the order through the payment processing system, if the product or service is not available for immediate shipment or fulfillment. (This rule applies to all methods of processing credit card payments, including over-the-counter transactions, telephone and mail orders, and Internet transactions.) The "hold" shall be released when the order is shipped or fulfilled. The settlement date may not be more than seven (7) days from the authorization date.

.109 Under generally accepted accounting principles (GAAP), credit card "sales" revenue is recognized when the customer's order has been fulfilled or shipped and the exchange is completed. Credit card revenues associated with licenses and fees are recognized upon receipt. For more information on revenue recognition, refer to **OAM 15.35.00**, Revenues and Receivables.

Deposit/Settlement

.110 Unless an exception is received by the agency, all credit card transactions must meet the deposit requirements of **ORS 293.265**.

.111 Credit card terminals: The daily receipts totals from all credit card processing devices must be printed and used to settle transactions at the end of each business day. Transactions settled before 5:00 p.m. will be posted to the agency's account at OST at midnight.

.112 DAS SecurePay or other payment processor: Daily transaction batches must be submitted before 5:00 p.m.

.113 Transactions settled before 5 p.m. will be posted to agency accounts the next business day if there are no changes/errors in the normal daily processes.

Reconciliations

.114 Daily Reconciliation: The total dollar value of each day's credit card receipts must be compared with and reconciled to the underlying transaction records of goods, licenses, etc., sold or issued.

a. Total credit card receipts from all systems must be reconciled to the total dollar value of the underlying transaction records (i.e., the number of products sold or licenses issued multiplied by applicable unit prices).

b. If the total credit card receipts do not agree to the total dollar value of the underlying transaction records, a transaction-by-transaction analysis must be performed to locate the difference.

c. Differences must be identified and corrected prior to clearing the deposit.

.115 Bank Reconciliation: The daily total for credit card receipts must be reconciled to the daily treasury statement received from OST, and the daily treasury statement must be reconciled to the Statewide Financial Management Application (SFMA**)** or the agency's cash management system.

Small volume transactions may be reconciled on a less frequent basis, such as weekly, but not less than once a month.

.116 Inventory Reconciliation: Settlement files must be reconciled with inventory records and/or customer databases on a regular basis.

Merchant Fees and Expense Recognition

.117 Merchant fees for all Visa and MasterCard transactions are deducted monthly from agencies' accounts at OST. Merchant fees associated with the Discover Card program are billed separately. Regardless of the method, agencies must review their US Bank Merchant Statements to ensure that the amounts charged for merchant fees are appropriate.

.118 For accounting purposes, merchant fees are recognized as an expense by recording them in comptroller object 4730. The related credit card revenue is recorded at the gross amount. For more information on expense recognition related to merchant fees, refer to **OAM 15.40.00.PO**, Expenses, Expenditures and Payables.

Refund Policy

.119 No cash refund shall be processed as the result of a credit card transaction including, but not limited to cash back requests, returned or undeliverable product, or an otherwise cancelled transaction.

a. The amount charged to the card must be fixed by the amount of the transaction.

b. Credits (refunds) must be issued to the same credit card used to process the original purchase transaction.

c. If the original credit card has been cancelled or has expired, a warrant or check refund may be issued upon receipt of a copy of the credit card reject document.

d. The agency's credit (refund) policy must be clearly displayed or otherwise communicated at the time of the initial transaction.

Chargebacks

.120 A chargeback is the reversal of the dollar value, in whole or in part, of a particular transaction by the card issuer to the state agency that originally processed the transaction. Chargebacks generally arise from customer disputes, fraud, processing errors, authorization issues and non-compliance with copy requests. It is recommended that agencies respond immediately to chargebacks and copy requests. Refer to the MTOS/MOR for further information and appropriate actions.

Segregation of Duties

.121 An adequate segregation of duties increases the likelihood that unintentional and intentional errors, including fraud, will be prevented or detected on a timely basis.

.122 Typical credit card functions that must be performed by separate individuals*, whenever possible*, include the following:

a. Processing the payment/authorization
b. Processing voids
c. Processing credits and refunds
   - Identifying credits

- Approving credits
- Issuing credits

d. Settlement
e. Handling billing and settlement errors
f. Reconciling

Credit Card Records Exempt from Public Disclosure

.123 All paperwork, records, receipts, card imprints, electronic data, etc., containing information provided to, obtained by or used by a public body to authorize, originate, receive or authenticate a transfer of funds, including but not limited to a credit card number, payment card expiration date, password, financial institution account number and financial institution routing number are exempt from disclosure under ORS 192.410 to 192.505 unless the public interest requires disclosure in the particular instance. **ORS 192.501(27) – Public Records Law**

Record Retention Requirements

.124 In general, copies of credit card receipts and supporting documentation must be retained by state agencies for 6 years (or in accordance with current archive requirements). However, copies of credit card receipts containing more information about a customer than the customer's name and five digits of the customer's card number must be destroyed on or before the sooner of:

a. The date the image of the copy is transferred onto microfilm or microfiche; or

b. Thirty-six (36) months after the date of the transaction that created the copy (**ORS 646A.204**).

Safeguarding Credit Card Records and Files

.125 Any agency that owns, maintains or otherwise possesses data that contains a consumer's personal information, including credit card information, must develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the personal information, including secure disposal of the data, in accordance with the Oregon Identity Theft Prevention Act (Oregon Laws 2007, Chapter 759).

.126 An agency shall be deemed to have met the requirements of the Oregon Identity Theft Prevention Act, if the agency is subject to and complies with:

a. Regulations promulgated pursuant to Title V of the Gramm-Leach-Bliley Act of 1999 (15 U.S.C. 6801 to 6809), as the act existed on October 1, 2007.

b. Regulations implementing the Health Insurance Portability and Accountability Act of 1996 (45 C.F.R. parts 160 and 164), as the act existed on October 1, 2007.

.127 An agency shall also be deemed to be compliant with the Oregon Identity Theft Prevention Act, if it implements an information security program that includes these safeguards:

a. Administrative safeguards such as the following, in which the agency:

- Designates one or more employees to coordinate the security program;
- Identifies reasonably foreseeable internal and external risks;
- Assesses the sufficiency of safeguards in place to control the identified risks;
- Trains and manages employees in the security program practices and procedures;

- Selects service providers capable of maintaining appropriate safeguards and requires those safeguards by contract; and
- Modifies the security program in light of business changes or new circumstances.

b. Technical safeguards such as the following, in which the agency:

- Assesses risks in network and software design;
- Assesses risks in information processing, transmission and storage;
- Detects, prevents and responds to attacks or system failures; and
- Regularly tests and monitors the effectiveness of key controls, systems and procedures.

c. Physical safeguards such as the following, in which the agency:

- Assesses risks of information storage and disposal;
- Detects, prevents and responds to intrusions;
- Protects against unauthorized access to or use of personal information during or after the collection, transportation and destruction or disposal of the information; and
- Disposes of personal information after it is no longer needed for business purposes or as required by local, state or federal law by burning, pulverizing, shredding or modifying a physical record and by destroying or erasing electronic media so that the information cannot be read or reconstructed. The agency may contract with another person engaged in the business of record destruction to dispose of personal information in a manner consistent with this paragraph.

.128 Any media (paper, electronic, or other) containing confidential cardholder information must be protected from unauthorized access and/or disclosure at all times. Backup media must likewise be securely stored. Paper documents containing confidential information must be stored in secure areas and/or in locking cabinets. Procedures to ensure the security of the keys or other locking mechanisms are also required.

.129 Networks or other devices, including point-of-sale terminals, used to store, process or transmit confidential credit card information collected from customers must be secure. Agencies must comply with the ISO/IEC 27002 Standard or the security architecture component of the Statewide Technical Architecture standard. ISO/IEC 27002 is an international information technology management standard that provides a generic set of best practices for use by those involved in initiating, implementing, or maintaining information security in an organization. The controls addressed by these standards include, but are not limited to, adequate physical and logical access security such as firewalls, data storage and transmission encryption, limited access to computer hardware, hardening servers, and regularly changed strong passwords.

Security Breach and Notification Requirements

.130 Under the Oregon Identity Theft Prevention Act, any agency that maintains personal information, including credit card information, of Oregon consumers must notify its customers if computer files containing that personal information have been subject to a security breach. The notification must be done as soon as possible, in one of the following ways:

a. Written notification.

b. Electronic, if this is the customary means of communication between an agency and its customers.

c. Telephone notice, provided that the agency can directly contact its customers.

.131 If an agency can demonstrate that the cost of notifying customers would exceed $250,000, that the number of those who need to be contacted is more than 350,000; or if the agency does not have the means to sufficiently contact consumers, the agency may give substitute notice. Substitute notice consists of:

a. Conspicuous posting of the notice or a link to the notice on the agency's website, if one is maintained, and

b. Notification to major statewide Oregon television and newspaper media.

.132 Notification may be delayed if a law enforcement agency determines that it will impede a criminal investigation.

.133 If an investigation into the breach or consultation with a federal, state or local law enforcement agency determines there is no reasonable likelihood of harm to consumers, or if the personal information was encrypted or made unreadable, notification is not required.

.134 If the security breach affects more than 1,000 consumers, the agency must report to all nationwide credit-reporting agencies the timing, distribution, and the content of the notice given to the affected consumers.

.135 Any state agency that is subject to and complies with the notification regulations or guidance adopted under Gramm-Leach-Bliley Act meets Oregon's requirements. However, if the breach involves the personal information of employees, the agency must follow Oregon's notification requirements.

.136 Agency resources, including best practices, checklists, sample notification letters and other tools, are available at the following websites:

a. Department of Consumer & Business Services: http://dfr.oregon.gov/Pages/index.aspx

b. Department of Administrative Services, Enterprise Information Strategy and Policy Division, Enterprise Security Office: http://www.oregon.gov/DAS/OSCIO/Pages/Security.aspx

Compliance with Payment Card Industry Standards

.137 Agencies that store, process or transmit cardholder information associated with credit card transactions must also comply with applicable industry data security standards. Visa, MasterCard, American Express, and Discover card brands require compliance with the Payment Card Industry Data Security Standard (PCI-DSS). The PCI-DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. **Failure to comply with industry standards may result in fines and/or revocation of credit card acceptance.**

.138 State agencies are required to implement a credit card processing system that does not store the following sensitive authentication data subsequent to authorization of the transaction:

a. The full contents of the magnetic stripe on the back side of the credit card.

b. The card validation code or value (the three-digit or four-digit number printed on either the front or back of the credit card).

c. The personal identification number (PIN) or the encrypted PIN block.

.139 The PCI-DSS also requires entities to develop internal policies and procedures that address credit card handling from the time information is received through its secure disposal. Examples of policy areas include:

a. Credit card processing procedures for agency staff and supervisors.

b. Access to credit card systems and information.

c. Security policy for credit card transactions.

d. Incident response plan for data breaches.

e. Storage of sensitive information, data retention and disposal policy.

.140 Agencies that accept credit cards as a payment option should work with OST to ensure they are PCI-DSS compliant and have successfully mitigated the risks associated with this payment option.

Third Party Service Organizations

.141 Third party service organizations that provide storage, processing, or transmission services and/or applications to state agencies associated with credit card transactions must be prequalified by the Office of the Treasurer (OST). Prequalification provides assurance that these vendors have met minimum industry and state security, interface, and depository requirements. In addition, OST will require an annual requalification to ensure that all approved vendors remain qualified. For more information on third party vendor requirements in connection with credit card transactions, refer to **OST Policy 02 18 14.PO**.