

State of Alaska Merchant Card Acceptance Guidelines

The State of Alaska Department of Revenue Cash Management Section administers the Merchant Card Acceptance Contract on behalf of the State. The State has a contract with U.S. Bank to provide merchant card processing services from October 2010 through October 2015, with two one year options. Elavon is a payment platform and wholly owned subsidiary of U.S. Bank. This document outlines the steps to establish new merchant locations. Please begin by contacting the Cash Management section:

Jesse Blackwell, Accountant IV, 907-465-3699, jesse.blackwell@alaska.gov

The following reference documents will be provided to you in a zip file:

- ✓ Add Location Form
- ✓ Chargeback Reason Codes
- ✓ Completing the SAQ
- ✓ Credit Card Security Policy
- ✓ Interchange Reference
- ✓ Merchant Card Acceptance Fee Schedule
- ✓ Merchant Connect Premium User Form
- ✓ MOG (Elavon Merchant Operating Guide)
- ✓ PCI SSC Quick Reference Guide
- ✓ Retained Fees and Bankcard Service Fees (HB 108 Sec. 28)
- ✓ SAQ-Scanning Chart
- ✓ Test Transaction
- ✓ Virtual Merchant User Guide
- ✓ Visa-MC No Signature Requirements

Other helpful references and contacts:

- Cash Management Section email cashmgmt@alaska.gov
- Cash Management WEB Site
<http://www.revenue.state.ak.us/treasury/programs/programs/index.aspx?70000>
- Charge backs dept (US Bank/Elavon): 866-600-5008 or email: chargebacks@elavon.com and disputeresolution@elavon.com
- "Code 10" security concerns for a specific card: 866-401-4852 and ask for "Code 10"
- Customer Service (US Bank/Elavon): 800-725-1245, option 1 or email: custsvc@elavon.com
- Customer Service after hours support (US Bank/Elavon): 800-777-7240
- InternetSecure: 866-638-8789 (press 3 to page on-call emergency support)
- Merchant Implementation and Training (US Bank/Elavon): 866-451-4007
- PCI DSS site <https://www.pcisecuritystandards.org/>
- Software Support (US Bank/Elavon): 800-377-3962, option 2, option 2
- Supply orders: 800-725-1245, option 8, ext. 8950
- Voice authorization (US Bank/Elavon): 866-401-4852
- Weekend support: 800-725-1245, option 1

Merchant Demographics for your department

Review the existing merchant demographics for the locations within your department that accept credit card payments from your constituents. Cash Management can provide you with the current merchant demographics for your department. The spreadsheet includes contact information for department finance officers, accountants in charge of credit card acceptance and IT staff. It also includes the credit card acceptance application for each merchant location (i.e. Virtual Merchant, InternetSecure, terminal card swipe), peripheral equipment and transaction volumes.

Please notify Cash Management of any changes to these demographics or contacts.

SAQ Scanning Chart and Merchant Card Acceptance Fee Schedule

The SAQ-Scanning Chart and the Merchant Card Acceptance Fee Schedule will assist you in determining which of card acceptance applications (i.e. processing environment) will best fit the business needs of your merchant locations.

The Merchant Card Acceptance Fee Schedule includes transaction fees, equipment and virtual terminal costs, and PCI DSS non-compliance fees. U.S. Bank and Cash Management encourage the purchase of equipment as a more cost effective method than leasing.

When determining the best card acceptance application it is important to consult with both the front end users and IT staff. Consider the business needs of the front end users and accounting staff. There may be connectivity issues or counter space limitations. Accounting staff may need specific reporting needs for reconciliation. IT staff should be consulted regarding any WEB based applications or IP connected devices. IT can contact Enterprise Technology Systems – State Security Office (ETS-SSO) regarding Internal Vulnerability Scans (IVS). Some card acceptance applications fall under the scope of PCI DSS scanning and others do not. The Card Acceptance Application Options document outlines the PCI DSS scope of each application.

Acceptance Application Options

VirtualMerchant (VM) is used for retail environments (face-to-face and mail order/telephone order). An administrator (i.e. Finance Officer) is set up in VM by Elavon. The administrator has the capability to add/delete/modify users as needed. The administrator handles password resets for users. Elavon provides phone training for VM, which takes approximately one hour. Magswipe card readers and receipt printers can be purchased to use with VM.

InternetSecure is used for WEB based applications. InternetSecure has two software application options: Merchant Direct and Merchant Link. Merchant Direct is payment page that is hosted by the

State. Merchant Direct can be used in both WEB based and retail environments (walk-in, mail order and telephone order). Merchant Link is a payment page that is hosted by InternetSecure. Merchant Link cannot be used in a retail environment.

If your department is adding a new WEB based application your IT staff will be provided with an InternetSecure developer's guide and web site audit requirements. Department of Administration Enterprise Technology Systems has a wiki site that was used during the statewide migration to InternetSecure: <https://wiki.state.ak.us/x/wwAkAg>

InternetSecure website:

- <https://www.internetsecure.com/Elavon/ShowPage.asp?page=HELP>

Confluence Wiki site:

- <https://wiki.state.ak.us/display/ets/US+Bank+Conversion+Reference+Guide>

Internet Secure developer's guide:

- <https://www.internetsecure.com/Elavon/ShowPage.asp?page=HELP>

Terminal swipe machines are offered with IP connectivity, dial up, and wireless connectivity. Elavon provides phone training for terminal swipe machines. If you need to order new equipment email your request to Cash Management. New equipment requests require an email approval from Finance Officers.

Add Location Form

The Add Location Form is used to provide U.S. Bank with the demographics (e.g. contact info, volumes, subaccount, equipment selection, etc) of a new merchant location. This information is used to build a merchant account ID (MID). Complete this form and email it to Cash Management. New merchant locations require an email approval from Finance Officers.

Merchant Connect Premium User Form

Merchant Connect Premium is used for reconciliation of revenues and fees. Statements can be downloaded and saved in PDF format. Cash Management encourages agencies to use this application in lieu of receiving paper statements. A print out of the summary page should suffice as back up for AKSAS entries.

Payment Card Industry – Data Security Standard

The PCI DSS, a set of comprehensive requirements for enhancing payment account data security, was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.

International. For information on PCI DSS, IT staff can reference: <https://www.pcisecuritystandards.org/>

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.

The State's merchants that transact data through PC devices or terminal swipes with IP connectivity are required to have: successful quarterly internal vulnerability assessment at the host level; successful annual external network penetration test; successful annual internal network penetration test. Your department IT staff can contact the State Security Office with any PCI DSS scanning or penetration questions.

The State's merchants are required to complete annual self assessment questionnaire's (SAQ's). SAQ's must be completed and emailed in pdf format to Cash Management for submission to U.S. Bank by the PCI Annual Validation Due Date for your department.

Completing the SAQ

One component of Payment Card Industry - Data Security Standard (PCI DSS) compliance is completing an annual Self Assessment Questionnaire (SAQ). "Completing the SAQ" outlines the process and provides information and guidance to complete the SAQ.

Credit Card Security Policy

The Credit Card Security Policy is a check list of policies a merchant must comply with in order to meet and maintain Payment Card Industry Data Security Standard (PCI DSS) requirements. The security policy must be distributed on an annual basis to all employees who access or handle card holder data.

Elavon Merchant Operating Guide (MOG.pdf)

This Merchant Operating Guide contains instructions for processing card transactions with Elavon and minimizing the risk of fraud. Failure to comply with these guidelines and suggestions may be considered a breach of the contract with U.S. Bank and may result in financial loss to the State.

Interchange Reference

The Interchange Reference is a comprehensive list of interchange categories and costs associated with each of them. A new interchange reference is issued by the card brands each fall and spring.

Best Practices to Qualify for Lowest Interchange Rates

Following is a best-practices bullet point list to lower the overall cost to accept credit card payments. This should be shared with front end users:

- Always enter/require AVS when a key entered transaction is carried out. Although CPS Retail 2 (emerging market) transactions don't require AVS, most other interchange type transactions do require AVS (corporate/commercial cards, Visa Signature Preferred, etc.) If there is a prompt that requests card present or not, if you select "Yes" the AVS must match the issuing bank or the transaction will downgrade. If you respond with "No", the AVS does not have to match for downgrade reasons.
- Always enter zero sales tax when the system (terminal or software) requires it. If it doesn't require it but you are able to automatically pass it/calculate it and send it, always send it. (e.g. software solution).
- Always settle on a regular 24 hour basis. (This needs to be within 24 hours from the auth time stamp of the first transaction in the batch or all transactions in the batch run the risk of downgrade). (pending special considerations, such as the delivery of a product prior to settlement of an authorization – this is only a case in MOTO or internet product situations – e.g. you order a product online, the merchant has up to 6 days to settle the transaction; meaning the order must be fulfilled in 6 days for the merchant to settle in a timely manner.)
- For face-to-face transacting swipe the card instead of hand keying the account number. There are certain transactions (typically international card types) which require a swipe in order to qualify at the best rate.
- If the terminal/software requests the Customer Code, please ask the cardholder for the information. If they do not have it, you may substitute the date in the format of DD/MM for the code. This is used for Interchange only reasons in Level 1 and 2 transactions.
- If the location is listed as MOTO (Mail Order /Telephone Order 90% keyed, 10% swiped) transactions require an invoice number to be submitted with each transaction. You may use the invoice number of your choice as long as it does not include any characters or letters.
- If you call Voice auth and Force a transaction authorization, it will automatically go to non-qualified.

Test Transactions

After the new MID is created and staff has received training on the new terminal, a test sale and test refund must be done before accepting card payments from constituents. A State purchasing card will be needed for the test transactions. Advise Cash Management when you are ready to process the test transaction and they will monitor the transactions through the banking process. See the TestTransaction.pdf for more details.

Refunds

When a location using a swipe terminal machine needs full card numbers to process a refund, they will need to contact the voice authorization department as listed on their Voice Auth sticker on their terminal.

They will need to provide the address of the location as well as:

1. Merchant Identification Number (MID)
2. Date of Transaction
3. Card number (truncated)
4. Amount
5. Authorization number

Charge Backs

If a customer disputes a charge you will receive notification of the charge back from Cash Management and the merchant account will be debited for the amount of the disputed transaction. These notices must be responded to within 25 days of issuance in order to accept or decline the charge back. The Merchant Connect Premium system will provide a "respond by" date. Refer to the chargeback_reason_codes.pdf document in the zip file.

1. Login to Merchant Connect Premium (MCP)
2. Pull up their chargeback record
 - a. My Reports > Chargebacks > Chargeback List > Select Date Range
 - b. Chargeback List Summary will appear. Click on one of the Case ID's.
 - c. Click on bottom link "Download Fax cover sheet"

If accepting charge back:

Once downloaded (it will open a new internet browser window), they will need to print it out, write "Chargeback accepted" or under "Optional comments", and either fax it back or email it to DisputeResolution@elavon.com.

If declining charge back:

Once downloaded (it will open a new internet browser window), they will need to print it out, write "Chargeback declined" or under "Optional comments", and either fax it back or email it to DisputeResolution@elavon.com. Include customer's signed receipt or other supporting documentation which validates the charge.

Retrievals

Retrievals are requests from the card holder for proof of their approval or presence (signed receipt) of the charge. Details can be obtained in Merchant Connect Premium.

1. Login to Merchant Connect Premium (MCP)
2. Pull up their chargeback record
 - a. My Reports > Retrievals > Retrieval List
 - b. Select Date Range (2 months in the past through current date)
 - c. Enter MID
 - d. Enter Case ID from the spreadsheet
 - e. Click Search
 - f. Click on Case ID for details

Retained Fees and Bankcard Services

Enrolled HB 108

Sec. 28. RETAINED FEES AND BANKCARD SERVICE FEES. (a) The amount retained to compensate the collector or trustee of fees, licenses, taxes, or other money belonging to the state during the fiscal year ending June 30, 2012, is appropriated for that purpose to the agency authorized by law to generate the revenue. In this subsection, "collector or trustee" includes vendors retained by the state on a contingency fee basis.

(b) The amount retained to compensate the provider of bankcard or credit card services to the state during the fiscal year ending June 30, 2012, is appropriated for that purpose to each agency of the executive, legislative, and judicial branches that accepts payment by bankcard or credit card for licenses, permits, goods, and services provided by that agency on behalf of the state, from the funds and accounts in which the payments received by the state are deposited.

(c) The amount retained to compensate the provider of bankcard or credit card services to the state during the fiscal year ending June 30, 2012, is appropriated for that purpose to the Department of Law for accepting payment of restitution in accordance with AS 12.55.051 and AS 47.12.170 by bankcard or credit card, from the funds and accounts in which the restitution payments received by the Department of Law are deposited.