Credit/Debit Card Processing Requirements and Best Practices

Adele Honeyman
Oregon State Treasury
Training Specialist

Oregon State Treasury
Relationship Management Team

What?

What do I need to know about excepting credit cards?

Who's involved, how it works, methods and practices for maximizing security and minimizing risks and what are the fees?

Follow Best Practices!

- Card Present Transactions
  - The card and cardholder are present at the point of sale (POS).
    - Retail Outlets
    - Gas Stations
    - Government agencies

- Card Not Present Transactions
  - Credit card transactions that are processed without ever seeing the card or cardholder.
    - Mail Order/Telephone Order (MO/TO)
    - Internet

    These are considered higher risk transactions compared to card present

Who?

Who are the participants in this process?

Oregon State Treasury
Relationship Management Team

Participants

Cardholder - Authorized user of payment card

Merchant - Provider of goods or services who is authorized to accept credit cards for electronic payment via the Internet and MO/TO

Card Issuer (Issuing Bank) - Financial Institution that provides a credit card to an individual for use

Merchant Bank - The financial institution that contracts with merchants to accept cards for payment of goods and services.

Card Associations - Visa and MasterCard are membership corporations each collectively comprised of thousands of banks worldwide. These banks pay membership fees to the associations, and are thus permitted to issue cards. They provide card products and establish the rules and regulations governing member participation in their programs.

Processors - Provide a point of connectivity for the Merchant to authorize and settle its credit card transactions through the appropriate payment network, e.g. Elavon

Oregon State Treasury

Rules

Terms of Service Guidelines:

- Authorize All Transactions
- Honor All Cards
- No Dollar Minimums and Maximums
- No Surcharging
- Convenience Fees
- No Cash Refunds
- Delivery of Goods and Services
- Compliance with Data Security Requirements
- Refund and Credit Policies
- Chargeback rules and regulations

*Make sure your staff is familiar with U.S. Bank's Merchant Terms of Service and Merchant Operating Guidelines

Card Benefits

<u>When following these rules…</u>

- You as the merchant will benefit:
  - Funding - Improves Cash Flow
  - Fee reduction
  - Improves Back Office Processes
  - Better Customer Service (convenience/preference)

Why?

Why do we need to know all this about credit cards?

Oregon State Treasury
Relationship Management Team

Protection!

Protect your agency AND your customer!

Common Risks include:

- FRAUD - Credit card fraud is something that can never be completely eliminated, but rather something that must be managed.
- Account Information Theft by Cyber-Thieves
- Customer Disputes and Chargebacks
- Protect your customers personal data.

What do we do?

So how do we process transactions safely and minimize our risks?

Best Practices

- Create or update agencies policies and procedures for credit card handling and processing.
- Safeguard Cardholder Data through PCI DSS compliance and annual risk assessment.
- Avoid Chargeback Loss
- Ensure staff are well trained and know how to properly process transactions.

Processing Transactions

- Three main steps in processing a transaction:

1. Authorization
2. Authentication
3. Settlement

Authorization

- Merchants must obtain approval from the Issuing Bank to process a transaction.
  - Authorization approval **does not mean** that the merchant is guaranteed payment. Approval only indicates that at the time the approval was issued, the card hasn't been reported stolen or lost, and that the card credit limit has not been exceeded.
- Authorizations protect merchants against fraud and chargebacks.
- Staff should receive one of the following responses during the authorization process.
  - Approved
  - Declined or Card Not Accepted
  - Call, Call Center, or Referrals
  - Pick Up
  - No Match
- When transaction is approved, a sales receipt is printed.
- When a negative or alert message is received, the response is displayed, a sales receipt is not printed.

Authorization Flow

1. Cardholder Purchase Request through Merchant site

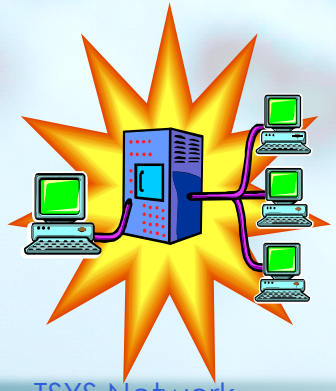
2. Authorization Request

7. Authorization Response

Elavon

3.

or



TSYS Network

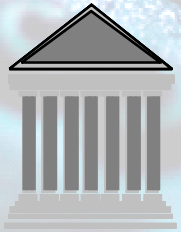
4. Authorization Request

VISA

or

MasterCard

5.



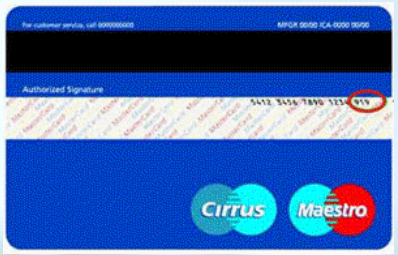
Card Issuing Bank

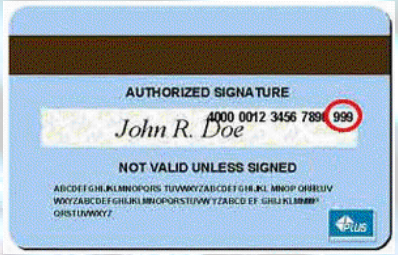
6. Authorization Response

Oregon State Treasury
Relationship Management Team

Authentication

- Involves the verification of the cardholder and the card.
- Examples include:
  - Address Verification Service (AVS)
  - Card Verification Value (CVV2 or CVC2)
  - Verified by Visa





Visa - Card Verification Value 2 (CVV2)
MasterCard - Commercial Verification Code (CVC2)

- The CVV2/CVC2 consists of the last three or four digits printed on the signature panel located on the back of all Visa and MasterCard cards.
  - Enhanced fraud protection may reduce amount of fraud-related chargebacks.
  - By checking the validity of the CVV2 or CVC2 code, the merchant will be able to differentiate between valid customers and fraud customers.

NOTE: This number is never to be recorded anywhere for any reason by anyone.

Settlement

- Once the product/service has been shipped or delivered to the customer, the merchant sends approved transactions to the Merchant Bank to facilitate funding to the merchant's DDA account and cardholder billing.

Settlement Flow

Merchant Settlement

Merchant batches transactions for settlement

Elavon

or

TSYS Network

usbank
Five Star Service Guaranteed

Elavon

State of Oregon Bank Account

Agency Accounts

Interchange Settlement

VISA

or

MasterCard

Card Issuing Banks

Cardholder Statement

Oregon State Treasury
Relationship Management Team

Card Present Transactions

Doing it Right at the Point of Sale

Card Acceptance Steps

These steps should be followed at the point of sale:

- Swipe the card to request the transaction authorization.
  - Hold the card or keep it in the presence of the customer through the entire transaction.
  - While the transaction is being processed, check the card's features and security elements to make sure the card is valid and has not been altered.
  - Obtain authorization and get the cardholder signature on the transaction receipt.
  - Compare the name, number, and signature on the card to those on the transaction receipt.
  - If you suspect fraud, make a Code 10 Call.

Always "Swipe the Stripe"

- On the back of every card there is a magnetic stripe.
  - Cardholder Name
  - Card Account Number
  - Expiration Date
  - Special security info designed to help detect counterfeit cards.
- When the card is swiped through the terminal, the info is electronically read and relayed to the card issuer, who then uses it as crucial input for the authorization decision.

Verify the Account Number

- Verify that the account number embossed on the front of the card is the same as the account number encoded on the card's magnetic stripe.
  - How you check the numbers depends on your POS terminal
    - Magnetic stripe number is displayed on the terminal or printed on the sales receipt. Match the last four digits of the account number on the card to those printed on the receipt.
    - Terminal may be programmed to check the numbers electronically
      - You will be prompted to enter the last four digits of the embossed account number, which will then be matched against the last four digits of the account number on the magnetic stripe.
- If the numbers don't match, you will receive a "No Match" message.
  - Make a Code 10 call

Card Won't Read – Why?

- Occasionally, you will swipe a card and the terminal is not able to read the magnetic stripe or perform an authorization. It usually means one of three things:
  - The terminal's magnetic stripe reader is not working properly
  - The card is not being swiped through the reader correctly.
    - Swipe card once in one direction, using a quick smooth motion.
    - Never swipe the card back and forth
    - Never swipe the card at an angle: this may cause a faulty reading.
  - The magnetic stripe on the card has been damaged or demagnetized.
    - Damage to card may happen accidently, but it may also be a sign that the card is counterfeit or it has been altered.

What to do if Card Won't Read

- Check card's security features to make sure the card is not counterfeit or has not been altered in any way
  (Refer to POS Reminder Card)

- Check terminal to make sure working properly and that you are swiping the card correctly.
  - If there appears to be a problem with the magnetic stripe, follow agency procedures.
    - You may be allowed to use the terminal's manual override feature to key-enter transaction data for authorization, or
    - You may need to call your voice-authorization center.

Key-Entered or Voice Authorized Transactions

- Make an imprint of the front of the card.
  - The imprint proves the card was present at POS and protects your organization from potential chargebacks if the transaction turns out to be fraudulent.
  - Imprint can be made on the sales receipt generated by the terminal or on a separate manual sales receipt form signed by the customer.

- Key-entered transactions are fully acceptable, but they are associated with higher fraud and chargeback rates.
  - Please contact OST if you see an increase in the number of key-entered or voice authorized transactions.

Requesting Cardholder ID

- Although Visa rules do not preclude merchants from asking for cardholder ID, e.g. driver's license, merchants cannot refuse to complete a purchase transaction because a customer refuses to provide ID.

Unsigned Cards

- An unsigned card is considered invalid and should not be accepted.
  - The words "Not Valid Without Signature" appear above, below, or beside the signature panel on all cards.
- You must take the following steps if you are given an unsigned card:
  - Ask for cardholder's official ID, e.g., driver's license, passport
  - Ask cardholder to sign the card.
    - Card should be signed within your full view
    - Check signature against cardholder ID

    Note: if customer refuses to sign the card is still invalid and cannot be accepted. Ask for another form of payment.

Code 10 Calls

- You should make a Code 10 Call whenever you are suspicious about a card, cardholder, or a transaction.
- The term "Code 10" is used so the call can be made at any time during a transaction without arousing a customer's suspicions.
- To make a Code 10 call:
  - Keep card in your possession during the call
  - Call and say, "I have a Code 10 authorization request."
  - You will then be asked a series of questions by your merchant bank and/or the card issuer.
  - Only respond by saying "Yes" or "No" calmly in a normal tone of voice.
  - Follow all operator instructions
  - If the operator tells you to pick up the card, ***do so only if recovery is possible by reasonable and peaceful means.***
- Note: staff can make Code 10 calls even after a customer leaves the store. This alert may help stop fraud at another location.

Reasons to Recover a Card

- Only recover a card if you have reasonable grounds for believing the card is being used fraudulently or is altered or counterfeit.
  - Card security features are missing, irregular, or appear to have been altered
  - Account number of magnetic stripe does not match the number embossed on front of card
  - You receive a pick-up response when card has been swiped, or you are instructed to recover the card during a Code 10 Call.

Card-NOT-Present Transactions

Mail Order/Telephone Order (MO/TO) Best Practices

Card-Not-Present Risks

- Typical Risks for Card-Not-Present Merchants
  - Fraud
  - Account Information Theft
    - Cyber-Thieves
    - Physical Site
  - Customer Disputes and Chargebacks

Managing the Risks

Your agency should address risk based on your business.

Key factors to consider include:

- How you will identify/authenticate your customers?
- What transaction data fields will customers be required to complete?
- What controls are needed to avoid duplicate orders?
- How you will validate both the card and cardholder during an Internet transaction or while processing a MO/TO transaction?
  - Do NOT write card information on separate sheet of paper. Input directly into Virtual Merchant
  - Do NOT restate card information – have customer repeat number

Fraud Prevention Best Practices

- Obtain an Authorization on all transactions
  - Authorization must occur before any merchandise is shipped or service performed. Be prepared to deal effectively with authorizations that are declined.
- Verify the cardholder and cards legitimacy
  - Compare card type and account number
  - Card Expiration Date
  - Card Verification 2 (CVV2/CVC2)
  - Verify the Cardholder's Billing Address with AVS
    - The Automated Verification Service (AVS) is an automated fraud prevention tool that allows card-not-present merchants to check a cardholder's billing address as part of the authorization process. Evaluate response code and take appropriate action.
- Safeguard Cardholder Data through PCI compliance
- Avoid Chargeback Loss

Suspicious Transactions

- Internet
  - Significant increase in failed card transactions
  - Multiple cards from a single IP address
  - Transactions originated from and/or shipped to International IP addresses
  - Shipping to a single address, but transactions placed on multiple cards
  - Multiple transactions on one card over a very short period of time
  - Multiple transactions on one card or a similar card with a single billing address, but multiple shipping addresses
  - Orders from Internet addresses at free e-mail services
- MO/TO
  - Hesitation
  - Rush Orders
  - Suspicious Shipping Address (P.O. or office address and International addresses)

Internet Transactions

Fraud Screening Tools - can be developed internally or acquired from third parties. These tools will identify high-risk transactions.

- An effective fraud screening program will suspend processing if a transaction:
  - Matches data stored in your internal negative files
  - Exceeds velocity limits and controls
  - Generates an AVS mismatch or CVV2/CVC2 no match
  - Matches other high-risk attribute. E.g. transactions associated with anonymous e-mail addresses, high-risk shipping addresses, or cards issued outside of the U.S. are considered high-risk.
- Develop effective and timely review procedures for investigating high-risk transactions.

Avoiding Customer Misunderstandings

Oregon State Treasury
Relationship Management Team

Web Site Requirements/Best Practices

- Your web site should include the following information to help avoid customer misunderstandings and downstream disputes.
  - Customer service contact information, including e-mail address or phone number
  - Privacy statement
  - Statement on web site regarding security controls used to protect customers
  - Complete description of goods and services
  - Order fulfillment and charge information
    - Provide information about delivery methods, delivery timeframe and when cards will be billed
    - Encourage cardholders to retain a copy of the transaction
  - Return, Refund and Cancellation Policy

Visa Rules for Returns and Exchanges

- Merchants are responsible for establishing return and adjustment policies. Clear disclosure can help you avoid misunderstanding and potential cardholder disputes. Visa will support your policies, provided they are clearly disclosed to cardholders **before** the completion of a transaction.
- Disclosure statements must be clearly printed on the face of the transaction receipt near the cardholder signature line or on applicable forms.
  - No Refunds or Returns
  - Exchange Only
  - In-Store Credit Only
  - Special Circumstances

The cardholder's signature on the receipt or invoice indicates acceptance of the agreed-upon terms.

Returns and Refunds

- If you allow returns, the refund must be made back to the card.
- Cash or check refunds are not allowed.
- Merchant will issue a credit to the Card on which the original purchase was made.
- Merchant will issue a Credit Transaction Receipt
- Amount cannot exceed the amount of the original Transaction receipt

Chargebacks

What is a chargeback?

- The process of taking back, or debiting, the merchant's credit card funds after the funds have been paid to the merchant. This occurs when a customer disputes a credit card transaction. The merchant must respond to the charge back and provide proof that the product or service was provided to the customer.

- Why do they occur?
  - Customer disputes
  - Fraud
  - Authorization issues
  - Processing errors
  - Non-fulfillment of copy requests

Chargeback Process Flow

1. **Cardholder -** Disputes transaction. Contacts card issuer with disputed information

2. **Card Issuer -** Returns transaction (charges it back) to merchant bank through Visa or MasterCard (electronically)

3. **Visa and MasterCard -** Reviews eligibility of transaction for chargeback. If appropriate, forwards chargeback to merchant bank (electronically)

4. **Merchant Bank -** Receives chargeback and resolves issue, or forwards to merchant

5. **Merchant (agency or university) -** Receives chargeback or copy request. If appropriate, and under certain conditions, may represent chargeback to its merchant bank.
   - If conditions are not met, merchant may have to accept chargeback
   - Chargebacks are electronically deducted from agency or university accounts.

6. **Merchant Bank -**Forwards documents of represented item to Visa or MasterCard (electronically)

7. **Visa and MasterCard -** Receives represented item and, if appropriate, forwards it to card issuer. (electronically)

8. **Card Issuer -** Receives represented item and, if appropriate, re-posts to cardholder's account. If chargeback issue is not appropriately addressed, card issuer may charge back the item a second time.

9. **Cardholder -** Receives information resolving initial dispute and may be billed for item. Cardholder may dispute presentment or item again if desired.

Oregon State Treasury
Relationship Management Team

Minimize Chargebacks

- Train staff and develop policies and procedures to ensure compliance with Merchant Terms of Service and Merchant Operating Guide
  - Do not complete a transaction if the authorization request was declined.
  - Ship merchandise before settling a transaction or have Elavon approve fulfillment and product delivery statement on web site.
  - Clearly post Refund, Return and Cancellation Policies
- Make sure customers can recognize your organizations name on their bills
- Chargeback monitoring – Elavon
- Consider using Risk Management Tools such as AVS and CVV2

Remedy Chargebacks

- Develop policies and procedures for handling copy requests, credits, and chargebacks.
  - Respond promptly when customers with valid disputes deserve credits.
  - Respond promptly to sales draft requests and chargebacks
    - Each step in chargeback cycle has a defined time limit
  - Send your merchant bank as much information as possible to remedy the chargeback.
    - With appropriate information, the merchant bank may be able to re-present the item to the card issuer.
  - Familiarize yourself with chargeback rights associated with use of Address Verification Service (AVS) and Card Verification Value 2 (CVV2).

Segregation of Duties

Segregation of duties when processing credit cards

"Segregation of Duties" in the procedure – we find this helpful as you make decisions about how you will set up users (right/permissions) in Virtual Merchant.

- http://www.oregon.gov/DAS/SCD/SARS/policies/oam/10.35.00.PO.pdf
- http://www.oregon.gov/DAS/SCD/SARS/policies/oam/10.35.00.PR.pdf

The separate duties it refers to are:

1. Processing the payment
2. Processing Voids
3. Processing credits and refunds
4. Settlement
5. Handling billing & settlement errors
6. Reconciling

Card Acceptance Fees

Card Acceptance Costs: Discount Rate

Full payment of the transaction amount is deposited to a Merchant's account. Associated card fees are either debited or billed to State of Oregon Merchants on a monthly basis.

- **Discount Rate**: The fee assessed to all merchant accounts for accepting and processing VISA/MasterCard Cards

- The discount rate is made up of three components:
  1. **Interchange Fees**
  2. **Assessments**
  3. **Processing Fees**

Card Acceptance Costs: Interchange

- VISA and MasterCard set and apply interchange fees
- Universally applied to all merchants
- Interchange is determined by:
  1. **Card Brand and Type**: Debit, Credit, Consumer, Commercial, International, Rewards, Corporate cards, etc
  2. **Merchant's Processing Environment**: Retail, Mail/Phone Orders, eCommerce, Government, Utilities, etc
  3. **Card Acceptance Method**: Swiped, key entered, online, etc.
  4. **Information sent with transaction**: Address Verification (AVS), CVV2, tax amount.
  5. **Timeliness:** Authorized versus settled

Card Acceptance Costs: Interchange

Interchange Fee

- Numerous Interchange Fee Programs
  - Visa > 75
  - MasterCard > 130
- Interchange Rates Vary
  - 1.03% + $0.15 to 3.25% + $0.10 (per transaction fee)
- Intended to provide balance to the system by addressing costs borne by Issuing Banks (reporting, bad debt, etc.)

Card Acceptance Costs: Assessments and Process Fees

- Assessment Fee
  - Moved to and retained by the card brand association (Visa/MC)
  - Visa = 0.0925%
  - MasterCard = 0.095%
  - Fee is consistent for all merchants

- Processing Fee
  - Retained by the Acquirer/Processor
  - Provides merchant funding, billing, statements, interfaces for authorizations, customer service, etc.

How to Get the Best Rates?

- For key-entered transactions: Include address verification during authorization (Don't need this when swiping the card)
- Include address verification during authorization
- Enter sales tax indicator, sales tax and order number
- Enter customer code/order number when prompted
- Ship product within 7 days of authorization; settle batch same day
- Settled amount must equal authorized amount

Resources

Dan Hough

737-2935 dan.hough@oregonstate.edu

Robert Monasky

737-0654 Robert.monasky@oregonstate.edu

Visa's Web Site – Merchant Info

http://usa.visa.com/merchants/index.html?scr=home