Transforming Idaho Government

Payment Processing 101

Idaho Association of Counties

September 9, 2020

999 West Main St., Suite 910, Boise, ID 83702 • 208-332-0102 • www.accessidaho.org

About Access Idaho

- Established in 1999 to manage State's website/services
- State contract good through June 2024
- County governments fall under State contract
- Located in downtown Boise
- 13 Employees
- IAC Associate Member for 10+ years

Electronic Payments: Where Do I Start?

Determine Merchant Account Ownership

- Merchant Account—a bank account that enables the holder to accept credit cards for payment.

- County-owned or 3rd Party?

Advantages of Using a 3rd Party Merchant Account

	County Account	3rd Party Account
Pass Fees to Customers		✓
Responsible for PCI Compliance		✓
Detailed Reporting		✓
Chargeback Responsibility		✓
Free Card Readers (swipe)*		✓
Counterfeit Liability (EMV) *		✓

Things to Consider

- Support—Who are they? Where are they? Are there costs?
- Contract commitment?
- Value (readers, reports, rates, refunds, etc.)?
- Minimum payment amounts?
- Other payment options (recurring payments, mobile, contactless)?
- Card types accepted?
- EMV functionality?

EMV FAQs

- **What is it?**
  - EMV® (Europay, MasterCard, and Visa)—global standard for credit and debit payment cards based on chip card technology.
- **Why does it exist?**
  - Designed to reduce *counterfeit* cards at *counter*
- **Is it mandatory?**
  - No!
- **Readers – types and costs?**
  - Depends on Merchant

Chargebacks FAQs

- **What the heck are chargebacks?**
  - The refund a credit card merchant pays to a customer after the customer successfully disputes a transaction on their credit card statement.

- **Who takes care of them?**
  - Depends on the Merchant

PCI FAQs

- **What does PCI stand for?**
  - Payment Card Industry (American Express, Discover, MasterCard and Visa)
- **Why does PCI-compliance matter?**
  - Outlines standards to reduce security vulnerabilities and help protect card holder data.
- **Does the County need to do anything to comply?**
  - Yes.

Quick Steps to PCI-Compliance

- Never store sensitive cardholder data (on computers, paper, etc.).
- Use a firewall on your network and PCs.
- Ensure wireless routers are password-protected & use encryption.
- Use “strong” passwords. Change default hardware and software passwords—most are unsafe!
- Regularly check computers for rogue software or “skimming” devices.
- Regularly inspect swipe card readers for tampering.
- Create an office culture of protecting cardholder data.

Questions/More Info?

Contact:

Rich Steckler
rich@accessidaho.org

Boise Area: 208-332-0102
Toll-Free: 877-443-3468
Cell: 208-860-4856