Sales Methods

H. DiMarchi

Contents

1 Introduction:

Webstore: Our plan to release an online webstore for our customers put us into a new tier of business. Webstores offer convenience, and enhance our ability to engage high volumes of customers.

Payment Methods: A customer will want to be able to pay for any order made on our webstore. We will need to support credit card processing to allow this. Multiple payment methods are available. The must be evaluated in terms of ease of customer use, cost, security and, relatedly, PCI compliance.

2 PCI Compliance:

2.1 Payment Card Industry Data Security Standard (PCI DSS):

The PCI DSS is a set of security standards that any organization transmitting or storing cardholder data must abide by. To be PCI compliant the organization must also secure validation of their compliance from the proper authorities. These twelve standards are grouped into six categories.

1. Build and Maintain a Secure Network
    - Install and maintain a firewall configuration to protect cardholder data
    - Do not use vendor-supplied defaults for system passwords and other security parameters
2. Protect Cardholder Data
    - Protect stored cardholder data
    - Encrypt transmission of cardholder data across open, public networks
3. Maintain a Vulnerability Management Program
    - Protect all systems against malware and regularly update anti-virus software or programs
    - Develop and maintain secure systems and applications
4. Implement Strong Access Control Measures
    - Restrict access to cardholder data by business need-to-know
    - Identify and authenticate access to system components
    - Restrict physical access to cardholder data
5. Regularly Monitor and Test Network

- Track and monitor all access to network resources and cardholder data
- Regularly test security systems and processes

6. Maintain an Information Security Policy

   - Maintain a policy that addresses information security for all personnel

Each of these requirements are further detailed by the PCI DSS to describe specific actions a PCI compliant organization must take.

2.2 Compliance Validation

Compliance validation is an involved process, requiring the participation of two entities.

2.2.1 Qualifid Security Assessor (QSA)

A QSA is an individual who has been certified by the PCI Security Standards Council. This individual can audit organizations for PCI compliance validation.

2.2.2 Internal Security Assessor (ISA)

An ISA is an individual who has been certified by the PCI Security Standards Council to perform PCI assessments for the organization they are representing. This process typically involves filling out the Self-Assessment Questionnaire.

3 Payment Methods:

3.1 Third-Party Payment Processor vs. Merchant Account

Merchant Account/Direct Processor We have the option of being issued a merchant accout by a direct processor. A direct processor is typically a bank. In this circumstance the merchant account is a unique type of bank account. This offers the greatest degree of stability. Account holds or terminations are very unlikely. When holds or terminations occur customers experience an interruption of service. This additional stability comes at the expense of a thorough and expensive intial vetting process, as well as high monthly and annual fees. Methods of this type are only recommended with approximately $5,000 - $10,000 in monthly transactions.

Third-Party Payment Processor Our second option is establishing an account with a third-party payment processor. These processors having many merchants that they aggregate into a single merchant account with a direct processor. Their clients avoid the intense vetting process involved in establishing a merchant account. Third-party processors require a minimal initial vetting process, charge minimal fees, and hold month by month agreements. This offers the most flexibility and immediate profitability. Third-party processors conduct extensive ongoing vetting of their clients. This increases chances of account holds or terminations.

3.2 Payment Gateways

All credit card processing will require a payment gateway, a interface customers can use to make their payments. Few direct processors offer a payment gateway. Developing an in house gateway is another cost to consider with the direct processor option. Many third-party processors offer their own polished payment gateway.

3.3 Potential Processors:

3.3.1 CDGcommerce

CDGcommerce is a PCI compliant merchant account provider, working as a middlde man between their clients and direct processors. Unlike most merchant account providers they do not charge setup, annual, or PCI compliaince fees. Additionally they offer two free payment gateway options. CDGcommerce charges a $10.00 monthly support fee, and offers a $15.00 month security service which includes $100,000.00 in data breach insurance. CDG charges a 1.95% + $0.30 fee on most cards. On corporate, international, and premium cards this jumps to 2.95% + $0.30. CDGcommerce's 24/7 customer service is highly rated, and the company holds an A+ with the Better Business Bureau.

3.3.2 Fattmerchant

Fattmerchant is a PCI compliant mercant account provider. Like CDGcommerce it is not a direct processor, but an intermediary for them. Also like CDGcommerce it does not charge setup, annual or PCI compliance fees. Fattmerchant offers 3 payment gateways at a monthly cost of $7.95. Fattmerchant charges $99.00 per month. Per transaction Fattmerchant charges a flat fee of $0.15. Flattmerchants 24/7 customer service is highly rated and the company holds an A+ with the Better Business Bureau.

3.3.3 Paypal

Paypal is a PCI compliant third-party payment processor. Paypal is nearly ubiquitous as a payment processor on webstores. Paypal requires customers to have a paypal account to process a transaction. It is likely that many clients have a paypal account and are comfortable using paypals proprietary gateway. This trust and confidence could increase the use of our webstore. Paypal does not charge any setup, annual, monthly, or PCI copliance fees. Paypal charges 2.9% + $0.30 per transaction. Paypal does not have highly rated customer support. However, because of the popularity of its use, solutions to most problems are readily found online. Paypal holds a B with the Better Business Bureau.

3.3.4 Square

Square is a PCI compliant third-party payment proessor. Square is best known for its smartphone card readers. Square is a popular third party payment processor and most customers will be familiar with it. Square does not charge any setup, annual, monthly, or PCI compliance fees. Square offers many tools that we could leverage. This includes their proprietary payment gateway. Additionally Square offers a basic, mobile-compatible, online store that syncs automatically with in-person Square mediated payments. Square charges 2.9% + $0.30 per payment. Square has decent customer support, but it is not available 24/7. Square holds an A+ rating with the Better Business Bureau.

3.3.5 Comparison

Processor	Type	Setup	Monthly	Transaction	24/7 Support
CDGcommerce	MA	$0.00	$10.00	1.95% - 2.95% + $0.30	Yes
Fattmerchant	MA	$0.00	$99.00	$0.15	Yes
Paypal	TPP	$0.00	$0.00	2.9% + $0.30	No
Square	TPP	$0.00	$0.00	2.9% +$0.30	No

Comparison of various providers

4 Recommendations: