Handling e-Commerce Payments

Objectives

To ensure:

* Handle payments in a safe and equitable way for users of e-commerce systems
* Minimize fraud from cardholder not present (CNP) transactions
* Maximize privacy and trust for users of e-commerce systems
* Comply with all local laws and PCI (merchant agreement) standards

Compliance and Laws

If you are a e-commerce merchant, you must comply with all your local laws, such as all tax acts, trade practices, Sale of Goods (or similar) acts, lemon laws (as applicable), and so on. You should consult a source of legal advice competent for your jurisdiction to find out what is necessary.

If you are a credit card merchant, you have agreed to the credit card merchant agreements. Typically, these are extremely strict about the amounts of fraud allowed, and the guidelines for “cardholder not present” transactions. You must read and follow your agreement.

If you do not understand your agreement, you should consult with your bank’s merchant support for more information.

PCI Compliance

To comply with the most current regulations concerning credit cards, you must review the PCI Guidelines and your merchant agreement. In brief, here are the twelve requirements you are required to use if you are going to handle credit card payments:

|  |  |
| --- | --- |
| Build and maintain a secure network | Install and maintain a firewall configuration to protect data |
|  | Do not use vendor-supplied defaults for system passwords and other security parameters |
| Protect Cardholder Data | Protect stored data |
|  | Encrypt transmission of cardholder data and sensitive information across public networks |
| Maintain a Vulnerability Management Program | Use and regularly update anti-virus software |
|  | Develop and maintain secure systems and applications |
| Implement Strong Access Control Measures | Restrict access to data by business need-to-know |
|  | Assign a unique ID to each person with computer access |
|  | Restrict physical access to cardholder data |
| Regularly Monitor and Test Networks | Track and monitor all access to network resources and cardholder data |
|  | Regularly test security systems and processes |
| Maintain an Information Security Policy | Maintain a policy that addresses information security |

OWASP is mentioned in the “Develop and maintain secure systems and applications” requirement.

Develop web software and applications based on secure coding guidelines such as the Open Web Application Security Project guidelines. Review custom application code to identify coding vulnerabilities. See www.owasp.org - “The Ten Most Critical Web Application Security Vulnerabilities.” Cover prevention of common coding vulnerabilities in software development processes, to include: …

This Guide is now the best source of information on securing your applications. Although useful, the OWASP Top 10 is designed to be a start on improving your application’s security, not a complete reference. The Top 10 is (at the time of writing) in the process of being updated.

Handling Credit Cards

Every week, we read about yet another business suffering the ultimate humiliation - their entire customer's credit card data stolen... again. What is not stated is that this is often the end of the business (see CardSystems being revoked by Visa and AMEX in the *Further Reading* section). Customers hate being forced to replace their credit cards and fax in daily or weekly reversals to their bank’s card services. Besides customer inconvenience, merchants breach their merchant agreement with card issuers if they have insufficient security. No merchant agreement is the death knell for modern Internet enabled businesses.

This section details how you should handle and store payment transactions. Luckily, it is even easier than doing it the wrong way.

Best Practices

* Process transactions immediately online or hand off the processing to your bank
* Do not store any CC numbers, ever. If they must be stored, you must follow the PCI guidelines to the letter. We strongly urge you to not store credit card details.
* If you are using a shared host for your site, you cannot comply with the PCI guidelines. You must have your own infrastructure to comply with the PCI guidelines.

Many businesses are tempted to take the easy way out and store customer's credit card numbers, thinking that they need them. This is incorrect. Do not store credit card numbers.

Auth numbers

After successfully processing a transaction, you are returned an authorization number. This is unique per transaction and has no intrinsic value of its own. It is safe to store this value, write it to logs, present it to staff and e-mail it to the customer.

Handling Recurring payments

About the only business reason for storing credit card numbers is recurring payments. However, you have several responsibilities if you support recurring payments:

* You must follow the terms of your merchant agreement. Most merchant agreements require you to have original signed standing authorizations from credit card holders. This bit of signed paper will help you if the customer challenges your charges.
* It is best practice to encrypt credit card numbers. This as a mandatory requirement in the PCI guidelines
* Limit the term of the recurring payment to no more than one year, particularly if you have “Card holder not present” (CNP) transactions
* Expunge the credit card details as soon as the agreement is finished

The problem with encryption is that you must be able to decrypt the data later on in the business process. When choosing a method to store cards in an encrypted form, remember there is no reason why the front-end web server needs to be able to decrypt them.

Displaying portions of the credit card

PCI only allows the presentation of the first six (the BIN) or the last four digits. We strongly urge you to not display the credit card at all if it can be helped.

There are many reasons why tracing, sending or presenting a credit card number is handy, but it is not possible to present credit card numbers safely:

* If a large organization has several applications, all with different algorithms to present an identifying portion of the credit card, the card will be disclosed.
* Sending an email invoice is a low cost method of informing users of charges against their credit cards. However, e-mail is not secure
* For many workplaces, call centre staff typically consist of itinerant casuals with extremely high churn rates
* Logs are attacked not to eliminate evidence, but to obtain additional secrets.
* In countries with small numbers of banking institutions, the institutional BIN numbers are limited. Therefore, it is possible to guess workable BIN numbers and reconstruct the card number even if most of the card number has been obscured.

Most credit cards consist of 16 digits (although some are 14 or 15 digits, such as Amex):

XXXX XXYY YYYY YYYC

C is the checksum. X is the BIN number, which refers to the issuing institution. Y is the client's card number.

You must not store the CCV, CCV2 and PVV (or PIN Verification Value). These are a credit card validation field used by many payment gateways to protect against imprint fraud as the value is on the reverse of the card. Storing this value is not allowed as per sections 3.2.3 and 3.4.

For these reasons, it is strongly recommended that you do not present the user or your staff with open or obscured credit card numbers. but we recommend you do not display any digits of a credit card at all – just the expiry date.

Swiping cards

This section is not applicable to most web application developers, but bears repeating.

You are not allowed to double swipe a customer’s card. This is the common practice of swiping the card in the electronic funds transfer terminal and then in the point of sale system. This is partially to prevent customers becoming used to people swiping their cards multiple times, which is unfortunately, all too often the first step before the customer’s card is fraudulently duplicated or otherwise misused.

You are not allowed to store the contents of the magnetic stripe or the stored value chip.

Patching and maintenance

The PCI requires you to patch your systems within one month of the patch becoming available for any part of your system which helps process or store credit card transactions. You must have virus protection, and it must be up to date.

Reversals

There are two potential frauds from reversals: an insider pushing money from the organization's account to a third party, and an outsider who has successfully figured out how to use an automated reversal process to "refund" money which is not owing, for example by using negative numbers.

Reversals should always be performed by hand, and should be signed off by two distinct employees or groups. This reduces the risk from internal and external fraud.

It is essential to ensure that all values are within limits, and signing authority is properly assigned.

For example, in Melbourne, Australia in 2001, a trusted staff member used a mobile EFTPOS terminal to siphon off $400,000 from a sporting organization. If the person had been less greedy, she would never have been caught.

It is vital to understand the amount of fraud the organization is willing to tolerate.

Chargeback

Many businesses operate on razor thin margins, known as "points" in sales speak. For example, "6 points" means 6% profit above gross costs, which is barely worth getting out of bed in the morning.

Therefore, if you find yourself on the end of many charge backs after shipping goods, you've lost more than just the profit of one transaction. In retail terms, this is called "shrinkage,” but police refer to it as fraud. There are legitimate reasons for charge backs, and your local consumer laws will tell you what they are. However, most issuers take a dim view of merchants with a high charge back ratio as it costs them a lot of time and money and indicates a lack of fraud controls.

You can take some simple steps to lower your risk. These are:

* Money is not negative. Use strong typing to force zero or positive numbers, and prevent negative numbers.
* Don't overload a charge function to be the reversal by allowing negative values.
* All charge backs and reversals require logging, auditing, and manual authorization.
* There should be no code on your web site for reversals or charge backs
* Don't ship goods until you have an authorization receipt from the payment gateway
* The overwhelming majority of credit cards have a strong relationship between BIN numbers and the issuing institution's country. Strongly consider not shipping goods to out-of-country BIN cards
* For high value goods, consider making the payment an over-the-phone or fax authority.

Some customers will try charge backs one time too many. Keep tabs on customers who charge back, and decide if they present excessive risk

Always ask for the customer's e-mail and phone number that the issuing institution has for the customer. This helps if other red flags pop up

A 10 cent sign is worth a thousand dollars of security infrastructure. Make it known on your website that you prosecute fraud to the fullest extent of the law and all transactions are fully logged.

Further Reading

* Visa and AMEX revoke CardSystems for PCI breaches:
* AMEX, Visa, Mastercard, Discover, JCB, Diner’s Club – Payment Card Industry  
  Payment Card Industry (PCI) Data Security Standard  
  <http://www.visa-asia.com/ap/center/merchants/riskmgmt/includes/uploads/AP_PCI_Data_Security_Standard_1.pdf>   
  <https://sdp.mastercardintl.com/pdf/pcd_manual.pdf>
* Visa  
  *Cardholder Information Security Program*  
  <http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html>   
  *Account Information Security Program*  
  http://www.visa-asia.com/ap/sea/merchants/riskmgmt/ais.shtml  
    
  *Mapping CISP to PCI*  
  <http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_Mapping_CISPv2.3_to_PCIv1.0.pdf>