volusion®

# Your Key to Internet Security


One of the best parts of selling online is getting paid. While sharing your products with the world is satisfying, unfortunately, we all have bills to pay. Thus, ensuring you get as much income as possible from your online store is essential to maximizing your success. This means that you need to know how to accept payment from your customers in a safe, efficient manner.

That's why we put together this toolkit – to ensure that you're not duped by credit card fraudsters. In a world where identity theft, hacking and internet spying are on the rise, it's essential that you safeguard your business assets and customers.

**Here's what you'll learn:**

- **What are basic ways that hackers steal my information and how do I protect myself?**
- **How do I avoid getting scammed by credit card fraudsters when accepting payment?**
- **What does PCI certification mean and why is it important to my online safety?**

As the old saying goes, an ounce of prevention is worth a pound of cure. Once you have these questions answered, you'll be fully able to identify warning signs and take preventative measures to stay safe online. That way, you can have peace of mind and focus on selling more instead of worrying about your security.

Let's dive in!

# Chapter 1

## How do hackers steal my information? How do I protect myself?

Before we discuss **how** fraudsters access and steal your sensitive data, let's talk about **why**. In the darkest corners of the cyber world, there's a well-developed underground market that exchanges billions of dollars a year for access to sensitive data like names, credit cards, financial records and identification numbers. Thus, cyber criminals want to steal your information so they can sell it to someone else or use it for their own gain. In other cases, hackers simply want access to your computer and its files to help conduct highly orchestrated cyber attacks.

Luckily, it mostly takes a little knowledge and common sense to protect yourself. Of course, the key here is awareness. In this chapter you'll learn about **phishing scams, malware, botnets and keyloggers.**

## The connecting thread is spam

Regardless of method, the one idea that ultimately connects all malicious cyber activity is spam. Think of spam as the messenger that carries these deceptive items to your computer. In short, spam is unwanted messages that are sent in bulk and is unfortunately a fact of daily internet life. From April 2010 to July 2010, over 12.7 trillion spam messages were sent. In fact, spam composes approximately 89% of all email messages.*

But how do you spot spam? For email spam, your best bet is to look at the sender and the subject line. If you don't recognize the sender, or the subject line includes a strange offer, delete it immediately. The highest volume of spam is related to pharmaceuticals and prescription drugs, comprising 74% of all spam. The next highest level is product spam, which includes messages on a wide array of products. So if you see something like this in your inbox, run for the hills.

Spam is a major issue facing the online community, as it drains network resources across the globe. But much more important to the safety of your online business, spam is a favorite mechanism for hackers to send malicious code or pull tricks to steal your sensitive information.

**Symantec Intelligence Quarterly, April 2010 – June 2010*

## Phishing

While phishing is a cute name derived from a favorite outdoor pastime, it's actually a very devious and dangerous way for fraudsters to get your personal information. In a nutshell, phishing is a form of spam disguised as a trusted contact that acquires your sensitive data under false pretenses.

One of the most common examples is email correspondence from a sender that appears to be your bank. In the email it asks you to "confirm your account details" or your "account will be terminated." Then, once you click on a link, it takes you to a legitimate looking website with fields for you to submit your account information. Unbeknownst to you, your very personal information has just fallen into the hands of an identify thief.

Phishing is one of the toughest internet scams to combat because it appears to come from a trusted source. More sophisticated attempts include legitimate looking email addresses, replicas of company logos and fully replicated website design. Even worse, most phishing schemes send you to a site with the same domain as a trusted company. In short, these guys are good.

Fortunately, there are several ways you can protect yourself. First, it's recommended that you invest in an antivirus and security software to protect your computer. Additionally, update your computer with any security enhancements. But more specific to phishing attacks, keep the following in mind:

- **Be skeptical of any requests for information.** Most legitimate companies won't ask you to submit sensitive data via email, especially banks or credit cards. If you receive an email like this, call the company in question and ask for further clarification.

- **Watch out for generic greetings.** Phishing schemes are based on lists of thousands of email or IP addresses. With this many fields, it's very difficult for imposters to know your name. Thus, pay attention to the greeting – if it says something very generic like "Dear valued customer," there's a heightened risk for phishing.

- **Don't believe ominous threats.** Your bank, credit card or favorite company isn't going to cancel your account or charge you extra fees over email. Most cancellation notices, late fees and strong transactions occur via direct mail or over the phone. If you receive a message like this, again, contact a company representative personally.

- **Look for contact information.** Most phishing schemes don't include additional contact information, like a phone number or physical address, because they're nonexistent.

- **Pay attention to spelling and grammar.** While these scammers might be technically savvy, they often tend to reside in foreign countries. Thus, pay special attention to spelling and punctuation – often times these disguised websites and email messages are full of typos.

The main defense mechanism against phishing is to be aware of this threat. Now that you know the signs, you're much better equipped to identify these attempts. Unfortunately, not everyone is as wise – phishing attacks continue to become more sophisticated and widespread. Thus, you're encouraged to do your part by reporting any phishing attacks to the proper authorities. Here's a few you can rely on:

- Anti-Phishing Working Group
- Google – Report Phishing
- U.S. Computer Emergency Readiness Team

Next up, we'll discuss how to protect yourself from malicious code, or malware.

# Malware

Another tactic wildly accepted by internet scammers utilizes a practice of installing devious software on your computer without your knowledge. This malicious software, or malware, can cause effects ranging from annoying popup ads to taking over complete control of your computer operations. The National Cyber Security Alliance (NCSA) reports that malware is the number one online security threat to small businesses. And to make things worse, attacks against small businesses are on the rise due to known vulnerabilities in networks.

There are four types of malware to be cognizant of: spyware, viruses, worms and Trojan horses.

## Spyware

The definition of spyware is pretty self explanatory – it's malware that tracks your computer usage to collect information about you without your knowledge. Most frequently, spyware monitors your Internet usage habits and reports it back to a database. This information is then fed to unethical online advertising businesses to target ads and gather behavioral data for research purposes.

Some forms of spyware, called adware, will go a step further by taking your internet usage habits and deliver ads specific to your interests based on other websites you've visited. Thus, the ringleader of the spyware attack is handsomely compensated for his or her efforts.

Spyware becomes particularly dangerous when used to capture your username and passwords, particularly for banking and credit card accounts. It can also wreak havoc on your computer by taking control of your operating system, slowing down everyday functionality and Internet connections.

## Visruses

Viruses make up the most well-known security threat among the general population, and rightfully so. This security threat encompasses all sorts of malware, but is technically defined as the following: a self-replicating computer program that spreads by inserting copies of itself into other executable code or documents.

In other words, viruses are in business to multiply themselves. For example, a virus can be included in an email attachment. Once opened, the virus is placed on your computer. That virus can then make its way to other documents that you would send to your friends and colleagues. Computer viruses can wreak havoc on your computer and others as it spreads, typically through email and shared attachments. Some viruses do nothing but replicate themselves, while others are designed to slow down your computer or access information.

The (only) nice thing about viruses is that they must be spread by a user. Much like the common cold, you're in the clear unless someone else passes the virus to you. Thus, by following steps to prevent and remove viruses, you can protect others from becoming infected.

## Worms

Worms are very similar to viruses but aren't quite as nice. The main difference is that worms are more powerful – they don't require human action to spread. Instead, they multiply automatically through a network. A worm is malware that's designed to copy itself from one computer to another by spreading itself to many computers without a human to help. Ultimately, this means that worms spread much faster viruses.

Computer worms have the same effects and objectives as viruses. However, since worms grow so quickly in volume, their negative impact on computers and users are usually much more severe.

## Trojan Horses

Remember the story of the Greeks taking Troy by hiding of soldiers in a horse disguised as a gift? Same story in the malware version. For our purposes, a Trojan horse is a delivery mechanism for malware. By themselves, they can't cause any damage – the real problem is the malicious code housed inside the Trojan horse.

Some of the most common forms of Trojan horses include: spammy email messages, free software downloads, downloadable videos, etc. Typically, fraudsters try to hook you in with a catchy offer, like "Watch this cute monkey dance!" Once you click on the link, the Trojan horse is opened and any type of malware is installed on your computer while you're distracted by the dancing monkey.

So what do you do to protect yourself, your business and your customers? Again, now that you know the basics, simply use your knowledge to make common sense decisions, like:

- Never open attachments or click on links in emails sent from someone you don't know or trust
- Always scan attachments for viruses and other malware before opening
- Don't download or run software and add-ons from unknown or suspicious sites
- Avoid installing pirated or unlicensed software
- Don't insert untrusted storage media and scan files before opening
- Only install trusted add-ons and don't click links in messages from unknown contacts
- Never download or buy software from pop-up messages and disregard unknown pop-ups alerting you of installed malware
- Use anti-virus software and configure it to perform frequent updates

Unfortunately, malware is everywhere and hackers use that to their advantage. If you believe that there's strength in numbers, pay special attention to what happens when machines individually infected with malware join forces. This special army creates what we call a botnet.

## Botnets

Essentially, a botnet is a large number of infected computers, together used to send spam and viruses around other networks. A botnet is also referred to as a "zombie army." This is because the ringleader of this nefarious network takes over an infected computer and operates it without your knowledge, ultimately turning your computer into a zombie.

So how is this army sent to battle? Here's how it works. First, a trojan horse is installed on your computer after you open an attachment or download a file. Then, the malware disguised by the trojan horse opens an Internet Relay Chat, or IRC. This portal allows the "botmaster" to take control of your machine and communicate with others. As the malware spreads to other computers, the botnet gains more strength.

Once the botnet is forceful enough to cause damage, the controller can begin sending out huge amounts of spam emails and files. And if the botnet continues to grow, it can send a massive number of requests to an unsuspecting network. This flood of messages can cripple the attacked network, making the resources completely unavailable to its intended users. This is known as a Denial of Service attack, or DoS. This type of malicious scheme is constantly taking place, affecting even the largest of companies.

How do these zombie armies affect you and your online store? Consider the following:

- Once infected, your computer's functions are considerably slowed.
- Your digital documents and passwords are highly vulnerable, leading to potential identity theft.
- The malware can install "keystroke loggers" to capture your personal information and sensitive data.
- The structure makes it appear that the botnet's illegal actions come from your machine.

The good news about botnets is that you already know how to prevent infiltration before it starts. Since the botmaster has to gain access to your computer through a Trojan horse, all you have to do is prevent the Trojan horse from entering your machine. Thus, by following the same steps to preventing malware attacks, you'll be zombie free.

This chapter summarized basic ways that fraudsters and identity thieves can access your information online, including phishing schemes, malware and botnets. The next chapter discusses an internet security topic that has a much bigger impact on your bottom line – credit card fraud.

# Chapter 2

## How do I prevent credit card fraud when accepting payment?

In recent years, online credit card fraud has become a highly profitable black market industry. While data security standards and online purchasing technology have responded with change, so have fraud methods. This cycle is likely to continue because too many online business owners remain unaware of how fraud works and the part they play in it. For every well-informed, responsible merchant, there are several who serve as easy targets for thieves. So to help protect yourself, here's some essential facts to keep in mind before you start processing transactions online:

**The internet is considered a higher-risk "card-not-present" environment where fraud is more difficult to prevent than in "card-present" environments.**

In a retail store, credit card transactions present little risk for a business owner because they require the physical presence of the card. If a card is lost or stolen, the cardholder quickly becomes aware that it's missing and notifies the credit card company, who declines all future authorization attempts. For this reason, relatively few successful purchases are made with lost or stolen cards.

Online transactions, however, use the card data as a substitute for the physical card, and it's unfortunately all too easy to separate the data from the card without the cardholder's knowledge. This means that the holder will remain unaware of the theft until unrecognized charges appear on their card statement. To make matters worse, many cardholders don't monitor their statements regularly or closely. Weeks or even months can pass before the theft is detected, leaving the card company to authorize all otherwise unsuspicious transactions in the meantime.

While it might seem reasonable to assume that the cardholder, the card company, or the processor would lose out in these situations, that assumption is incorrect. Fortunately, we all have ways to protect ourselves.

**Industry standards established by the associations (Visa, MC, Discover, AMEX) consider you, the merchant, responsible for processing fraudulent online credit card transactions.**

Since cardholders and issuers are powerless to detect and prevent most cases of online credit card fraud, they place the financial liability on merchants accepting the cards. This may seem unfair, but of all parties involved in a credit card transaction, you actually possess the most fraud prevention leverage.

Merchants like you often feel an unfounded sense of security when signing up for a card processing service, assuming that either the processor or the issuer will protect you from fraud during the "authorization" step. The name of this step is a bit misleading, however, because it implies accountability. It actually has a much different industry-specific application: authorization only verifies whether or not the transaction will exceed

the card's spending limit, and whether or not the cardholder has reported the card lost or stolen. Once a transaction passes these two simple tests, the issuer grants authorization and full liability transfers to the merchant. In cases where stolen card data is used, if the merchant mistakenly assumes it's safe to capture funds simply because they have been "authorized," the authorization actually serves to facilitate, rather than prevent, fraud.

Unfortunately, your processor can't protect you, either, since no processor has the manpower to perform detailed analysis of every transaction it processes. Your processor can only help you by teaching you how to protect yourself.

## You're subject to chargebacks

Issuers do monitor purchasing activity to varying degrees and can sometimes prevent fraud by declining authorization attempts with suspicious elements (unusual frequency of card usage, unusually high transaction amount, untrustworthy merchant, etc.), but their primary responsibility is to their cardholders, not to you.

If a merchant processes a transaction with a stolen credit card, the issuer usually reimburses the cardholder by debiting the processor. The processor, in turn, debits the merchant and assesses a standard chargeback fee specified in the service contract. In such cases, the processor will provide you, the merchant, an opportunity to reverse the chargeback, but it will often be too late for you to present a compelling case. The merchant will lose the transaction amount, the fee amount, and perhaps even the merchandise, if they're unable to recover it through their own efforts.

## Chargebacks can impact more than your monthly revenue

Since processors are liable for all chargeback restitution that their merchants cannot cover, they always reserve the right to impose funding conditions on merchant accounts to prevent loss. If you become a fraud victim, your processor may hold some or all of your transaction funds aside for a period of time in a "reserve account" that you can't access, regardless of your operating capital needs. This helps the processor cover its exposure in the event of future chargebacks to your account.

And because issuers provide cardholders up to six months to dispute charges, your processor can leave the reserve account in place for six months beyond your most recent transaction. In extreme cases, you may lose your right to process credit cards through your provider, or even find yourself blacklisted in a fraud control database, which could bar you from processing credit cards through any responsible provider.

## There are methods you can use to help significantly minimize your risk

The only foolproof way to prevent all potential fraudulent credit card activity on your website is to not accept credit card payments at all. But there's no need to go to such an extreme because you can drastically reduce your risk level by following some basic guidelines. Note that most of the effective fraud prevention methods available to you require order analysis prior to capturing funds.

# Here's some tips on how to prevent credit card fraud before it happens.

### Capture the CVV2 at checkout, and examine the response code.

The CVV2 is Visa's name for a 3-digit security code printed on the back of the card. MasterCard calls it the CVC2, and Discover and American Express call it the CID (on American Express cards, it is a 4-digit number printed on the face). Since it's not stored in the magnetic stripe or embossed on the card along with the number, expiration date, and cardholder name, it can't be stolen through most methods used to steal these other details. When your customer uses the correct security code, the likelihood that the physical card is in their possession is significantly higher.

### Be wary of unusually-high transaction totals.

If your average sale is $30 and you receive an order totaling over $1000, it may seem too good to be true because it probably is. A large volume order of your highest ticket items can make your mouth water, but this is the riskiest type of transaction to process, and should be treated with appropriate skepticism; if the transaction isn't legitimate, you stand to lose as much as you hoped to gain (and more).

### Be certain that the customer's Internet Service Provider is in reasonable proximity to the billing address.

You can check this by clicking the IP address above the billing address on the Order Details page. If, for example, the billing address is in Miami while the order was placed from an IP address obtained through an ISP in Indonesia, don't capture the funds or ship the product. Certain delivery methods allow mail forwarding to a different destination than the one you specify for shipment. Also, be aware that it's possible to spoof an IP address. This means that an IP match cannot rule out fraud, but an IP mismatch can confirm it.

### Watch for multiple failed order attempts.

While many consumers do use two or three cards on a regular basis, watch out for multiple attempts in which certain variables remain consistent while others change, such as a consistent IP address with different customer names, or a consistent credit card with different billing addresses.

### Be wary of suspicious-looking customer names.

Fraudsters will often take the time to steal the true cardholder's name and use it on the order to enhance the thoroughness of the deception, but since the correct cardholder name can't be verified at a glance and isn't required for a successful authorization, they may also take a shortcut and use a false name. Fortunately for you, these names often look just like what they are.

### Be conscious of the customer's email address.

Watch to see if an email address from an order contains random characters, especially if provided through a free service like Yahoo!, Gmail, or Hotmail. These accounts are easy to create, and anyone trying to scam merchants in this fashion is likely to have created some.

### Be wary of orders placed with email addresses that include a different name than the cardholder.

For example, if the cardholder is "Brian Smith" & the email address is robbie94226@gmail.com, ask yourself why "Robbie" has Brian's card, or why Brian is using Robbie's email address.

### Be wary of all international orders, especially ones from high-risk regions like Southeast Asia, the Middle East, Africa, Eastern Europe, and Central America.

Many countries in these regions are hotbeds of credit card fraud and are unlikely to ever supply you a legitimate sale. Orders from them may not even be worth the hassle of reviewing.

### Use your IP Firewall to block fraudsters from repeat attempts.

If you catch someone trying to defraud you once, use your IP firewall in your ecommerce software to deny them future access to your store.

### Call the phone number provided with the billing address.

Since a fraudster can still pose as the cardholder over the phone, this method won't always allow you to detect fraud, but nonworking numbers, non-answers, and suspicious conversations with thieves who are not so competent when confronted can help you rule out orders that have raised fraud suspicion for other reasons.

### Do a reverse lookup on the phone number or billing address.

You can use http://www.whitepages.com/reverse-lookup to verify the connection between the phone number and street address entered on an order. This is especially useful when the system verifies the address, but you're skeptical of the phone number.

### Request that the credit card company make a courtesy call to the cardholder to confirm the order.

If you're able to obtain the full card number by calling the billing phone number and you're still uncertain about whether you've spoken to the true cardholder, Discover (800-347-2000) and American Express (800-528-5200) can call the cardholder at the number stored in the account profile to confirm legitimacy of the order. Be prepared to provide your merchant number (Discover numbers are 15 digits and American Express numbers are 10 digits). You can also call Visa (800-847-2750) and MasterCard (800-622-7747) to obtain the issuing bank's phone number for this purpose.

### Always examine the billing address before shipment.

Since only the numeric portion of the street address is required to pass the address portion of a default system check, creative fraudsters can enter this variable in the shopping cart address fields in a manner that will pass the check but encourage you to ship to an unrelated address. Be suspicious of unusual address formats in either or both address fields. Also, watch out for fake/generic-looking addresses, such as "123 Main Street." Although thieves may not be able to receive the ordered merchandise at such addresses, they may simply be using your store as a testing ground for one or more stolen credit card numbers.

## Be especially careful with customers who request shipment to a different location than the billing address.

Although there is nothing inherently suspicious about such orders (since gifts are often purchased this way), this is the easiest way for a fraudster to use a stolen card to receive merchandise. To protect yourself, you can require these customers to pay by money order, wire transfer, or cashier's check prior to shipment, or you can use signature confirmation delivery methods. If you take the latter tactic, be sure to avoid "indirect signature" methods, which allow anyone at the location or at adjacent locations, even underage persons, to sign for the delivery. Also, be certain that your chosen shipment method doesn't allow use of a stored signature from a previous delivery. Signature confirmation can add to your expenses and cut into your profit margin, but it's far preferable to handing your merchandise over to a thief.

## Finally, use common sense.

If something about an order doesn't look or feel right, don't capture the funds or ship the merchandise. In this industry, merchants have to look out for themselves. When your liability is high, it's sometimes better to be safe than sorry. All successful banks and processors use this philosophy, and so should all merchants who want to succeed in ecommerce.

This chapter taught you basic truths of accepting payment online and detailed numerous ways for you to detect credit card fraud before facing the consequences. Now that you have this vital information in your pocket, the next chapter discusses the importance of PCI Certification to your online business and ecommerce provider, and what you need to do to remain certified by various credit card companies.

# Chapter 3

## What's PCI certification and why is it important to my online safety?

The internet is an ever-evolving medium, much like a conversation that can be modified by anyone in the world. Most participants hope to inform and enrich the lives of others, but some participants enter the arena with malicious intentions. This latter group is growing in number and strength, armed with more tools than ever before. Your online business must now focus on protecting itself and the sensitive information of your customers. This is where PCI certification comes into play.

## What does PCI mean?

The Payment Card Industry (PCI) is a joint creation of Visa, MasterCard, Discover and American Express. In response to the growing frequency and severity of credit card and identity theft, this organization created the PCI Data Security Standard (PCI DSS), with the overall goal of protecting credit card data wherever it may reside.

The Cardholder Information Security Program (CISP) was initiated and mandated by Visa in June 2001 by Visa. In 2004, these requirements were incorporated into the PCI DSS to establish industry wide standards for card security. These standards must be followed by both merchants and providers.

## Why is PCI Certification important?

Identity theft is a major issue that's growing exponentially. The FTC estimates that approximately nine million Americans have their identity stolen each year, a crime amounting to $45 billion. In September 2009, one hacker pleaded guilty to stealing over 170 million credit card and debit card numbers, the largest identity theft case in US history.

PCI compliance is critical for anyone doing business online, including the merchant and the customer. For the merchant, the penalties of using a non-PCI compliant provider can include:

- $500,000 in fines (per incident)
- Complete loss of ability to process card transactions
- Class-actions lawsuits
- $10,000 in monthly fines
- Major public relations crises

For the customer, credit card and/or identity theft is devastating. Dozens of calls must be made, dozens of forms must be filled and credit can be ruined. More important to your business, your customer has a new sense of mistrust that makes them weary to purchase with you online.

*Sources: Federal Trade Commission, Washington Post, Javelin Strategy and Research*

# What's the difference between compliance and certification?

PCI compliance indicates that a merchant simply follows the PCI DSS guidelines. This means that there's a wide spectrum of security measures that would qualify a business as compliant. Also, compliance is only measured once a year, so rapid-spreading malware and hacking innovations are not always addressed. In sum, there's a lack of accountability with compliance and it's no longer stringent enough to protect your most valuable asset – your business.

PCI certification, on the other hand, is a higher degree of guaranteed security. In order to be certified, a provider must make major investments in their servers and hardware to meet higher security standards. When this has taken place, there's a rigorous screening process to be listed on Visa's certification list. Additionally, PCI certified companies are required to have an independent auditor come to their physical location to thoroughly inspect the security implementation.

### The vast majority of shopping cart solutions hasn't reached the level of PCI certification.

Merchants using non-certified solutions face the greatest amount of risk because it's easier for hackers to access sensitive customer information. Most of these providers are unable to achieve certification because of the following:

- They don't have the necessary capital to complete certification requirements
- They aren't knowledgeable enough to configure and code certification requirements
- They don't meet Visa's minimum company size requirements

You can check the status of various providers on Visa's list at: http://usa.visa.com/download/merchants/cisp-list-of-pcidss-compliant-service-providers.pdf. If they aren't listed, your business is not adequately secured.

# What do I need to do to remain certified?

PCI certified solutions have completed the overwhelming majority of the work; however there are still measures that must be taken from the business level. In order to be fully certified at the merchant level, your team must do the following:

- Select a PCI certified solution.
- Complete the Self Assessment Questionnaire (SAQ) once a year.The SAQ is a list of questions about your website and current security practices.
- Complete a vulnerability scan through an approved scanning vendor (ASV) periodically throughout the year. Then, provide documentation that your site passed the scan.

You can find the SAQ and list of ASVs online at: https://www.pcisecuritystandards.org/.

# How do different ecommerce solutions fit in?

## Hosted Solutions

Using an ecommerce provider that is fully hosted and PCI certified provides the most efficient and cost effective method of achieving certification for your own website. This is because the provider has already completed the effort required to achieve this status, so your business automatically falls into this level of security certification.

Most hosted solutions are not PCI compliant or certified, so ensure your business inquires about the security level when searching for ecommerce providers.

## Open Source Solutions

Open source ecommerce solutions require hosting on your servers or procure hosting with another provider. This means that all measures to reach PCI certification fall under the responsibility of the business owner, which is a large capital and human resources investment.

## Licensed Solutions

Licensed ecommerce solutions also require your business to find a hosting provider, either in-house or from a third party. With this type of solution, your IT team must handle all certification efforts or pay a premium to be hosted with an entity that has reached this security level.

# Why Volusion?

Volusion is a fully hosted, fully PCI certified ecommerce provider, offering the highest level of security possible. The company also offers a 99.99% uptime guarantee with 100% redundancy of all network hardware, systems and data. In addition to being PCI certified, all sites are protected by dedicated, dual firewalls and equipped with leading proactive anti-virus tools. Your website is also placed on multiple servers, all housed in secure, unmarked facilities with 24x7x365 surveillance. Volusion is focused on safeguarding your online business so you can focus on growing it.

# Ready to get started?

Now that you're a master of online marketing, why not get started with your very own online store? Keep in mind that you don't have to perform all of the actions listed in this document out of the gate. As your business and knowledge grows, you can easily deploy these new tactics in a timeline that's comfortable for you. Better yet, there are tons of resources and professionals to provide assistance along the way.

Selling online is a fun, exciting process that allows anyone to fulfill their dream of becoming a business owner or satisfy a desire to extend their hobby to the masses, especially in this period of booming ecommerce growth. If this opportunity sounds interesting to you, it's time to turn your idea into reality with Volusion. You'll receive a fully hosted, award-winning shopping cart solution full of features needed to build, manage and grow a successful online business. Thousands of merchants have trusted their success to us, and this number is growing each day. Our customers enjoy peace of mind by experiencing 24x7x365, live Out of this World Support™ from our team of friendly ecommerce experts.

Ready to give it a try? Sign up for a **free 14-day trial** of our software – no credit card or obligation required.