

RezNEWS Feature Article

No one is immune from credit card Payment Card Information (PCI) compliance

Most people have heard the horrid stories about Internet hackers who compromise large databases and gain access to vast sums of personal information such as credit card numbers, social security numbers, medical histories, etc. In the past, Internet hackers have been successful in disrupting services on such websites as E-bay and Authorize.net (one of the largest online credit card gateways). The following **RezNEWS** feature article discusses the importance of Payment Card Information (PCI) compliance in the era of Internet hackers and identity thieves, and the role PCI compliance plays in avoiding security breaches within your business.

When smaller companies would ask if they were in danger they were often told not to worry about it. The logic was that hackers were only interested in larger, more lucrative corporations. The irony is that today the number one target for hackers and other fraudulent schemes are smaller businesses. There are several reasons why hackers now focus more on smaller companies. First, larger businesses have gotten better at protecting sensitive data. Second, smaller companies are easier targets. Today, most credit card fraud occurs in bars, restaurants, and in smaller businesses.

To protect credit card processing data, Visa and MasterCard have joined with other credit card providers to create standards for the protection of credit card data. As part of the Cardholder Information Security Program (CISP), banks, credit card processing gateways, software developers, and even small hospitality businesses must be PCI compliant. There are different levels of compliance depending on the number of transactions that a company processes per year. Banks and credit card processing gateways must be compliant at level 1 and level 2. Software developers must usually be compliant at level 3. Hotels, inns, and other hospitality businesses that process credit cards must be compliant at level 4.

RezNEWS Tip: Even smaller businesses must be PCI compliant. RezStream suggests you become aware of this requirement and proactively work toward compliance. Although the government may not knock on your door tomorrow, you *are* vulnerable to Internet hackers...today.

How do hospitality businesses become PCI compliant?

There are several things that smaller businesses must do to become PCI compliant. Here is a list of things that need to be completed.

- Use a validated software programs and validated credit card gateways.
- Make sure you process all credit card payments on computers designated for business use only. For example, allowing employees to download streaming music videos or engage in other personal behavior opens your business up to security intrusion possibilities.
- Make sure your computer network is behind a firewall. You don't need a Cisco firewall but you must have a basic firewall installation.
- Do not use default Windows passwords such as "password" to log into any computer.
- You must have anti-virus software installed on all machines and set to auto update.
- If you use a wireless network you must also ensure that it is secure and encrypted.

In addition to these items, you are required join a PCI compliance program that allows you to run security scans on your network. With that, you will also fill out a questionnaire that must be filed before you are officially PCI compliant. The complexity of this process increases if you have an Internet connection that is always on (as most businesses do).

There is no such thing as partial PCI compliance

There are many businesses who mistakenly think they will be compliant if they simply do the things on the PCI compliance list. Software developers must be compliant at a higher standard than businesses that just process credit cards. For example, for software developers to be PCI compliant they must:

- Use “strong” encryption of credit card numbers they store in databases.
- Not store swiped data from any credit card.
- Use SSL (secure socket layer), strong encryption, etc. when passing credit card numbers from their online booking engine into any desktop application.
- Not store security codes, or transfer security codes, in any database (security codes may only be used for imminent transactions).
- Full card numbers must not be displayed on invoices, in letters, etc.
- Full credit card numbers cannot be viewed without entering a user name and password.

Doing these things do not make a business PCI compliant. You must also go through the PCI program, self test, submit to third party on-site testing, and apply and be granted for PCI Record of Compliance (ROC). In addition, PCI compliance can be expensive, especially if you wait until you have a security breach to enter the program.

RezNEWS Tip: When you sign up for RezStream’s new credit card processing module you may also elect to enter into the PCI compliance program through RezStream’s partnership with Payment Processing Inc. The cost for this benefit is \$300 per year and entitles you to 24/7 technical help in becoming PCI compliant, access to online scan services, all questionnaires, and any other assistance you need in becoming PCI certified.

Conclusion

Larger businesses are scrambling to become PCI compliant; however, smaller companies also have a responsibility to be PCI compliant. It should be noted that it is not enough to “do everything that Visa and MasterCard require” to be PCI compliant. You must also go through the self-testing process and fill out extensive questionnaires. Furthermore, PCI compliance is an ongoing process; you have to continue to self-test and comply with other requirements of the program. While PCI compliance may not be glamorous, it is critical with hackers and identity thieves who would like nothing more than to steal a few thousand of your customer’s credit card numbers, and other information, for their own personal use.

About the author

Bill Mitchell is co-owner and Chief Operating Officer for RezStream. Bill has over 30 years experience in the hospitality industry with extensive knowledge in management and marketing for hotels, resorts, and bed and breakfasts. Bill is recognized nationally as a featured speaker and consultant for the hospitality industry.