REVENTION™

The Dangers of Not Being PCI Compliant

Dangers related to credit card processing online and in store.

Introduction

One of the most frequent questions asked by merchants today is what happens if my business is effected by a data breach. What does happen? Truthfully it varies depending on several factors which include but are not limited to the following; number of credit card numbers breached, the source of the breach, level of investigation and the merchants PCI compliancy status. If you are a validated PCI compliant merchant and are using a PCI complaint online ordering solution then your concern of being breached should be minimalized exponentially.

Brand Damage

If you are a successful restaurant you know the value of marketing. Marketing can be a mail out to potentials customers, an email, a loyalty promotion, even word of mouth. If someone has a bad experience at your restaurant they will absolutely share their bad experience with no less than 5 people. The same will happen if your customer's credit card number was skimmed, stolen, or hacked from your restaurant or from your online ordering site. On June 1, 2012 Courthouse News Service reported, A Six-Figure Breach at Five Guys. See article below.

http://www.courthousenews.com/2012/06/01/47017.htm

Non-Compliance Fines

The consequences of not being PCI compliant range from $5,000 to $500,000, which is levied by banks and credit card institutions. Banks may fine based on forensic research prompted by a potential breach. Credit card institutions may impose fines as a punishment for noncompliance. The information below is used by VISA as an example of costs related to a breach.

- $50—$90 fine per cardholder data compromised
- Suspension of credit card acceptance by a merchant's credit card account provider
- Loss of reputation with customers, suppliers, and partners
- Possible civil litigation from breached customers
- Loss of customer trust which effects future sales

These fines can be incurred regardless of the source of the breach.

Litigation Expenses

When a data breach occurs the question everyone wants an answer to is who is responsible. Consumers, merchants, and banks are searching for the responsible party. Merchants are an easy target for a legal action. If a merchant has not followed the PCI Data Security Standard it is not difficult to sue for damages. A restaurant group in Massachusetts was ordered to pay a $110,000.00 in civil penalties to the Massachusetts Commonwealth. On March 28, 2011 the judgment was signed. The original beach occurred in April 2009. Read more about the case.

Cyber Crime on the Rise

In a country where hackers steal personal data from computer systems almost daily, the public websites using such personal and financial data are at the highest risk ever for intrusion and potential data breach. The FBI has been strengthening its cyber operations over the past year, in fact, FBI Director Robert Mueller said that, "cyber security may well become our highest priority in the years to come." Locking the doors to protect your business from crime is no longer enough. Adhering to the PCI Data Security Standard (PCI DSS) requirements is more important than ever for both your business and the online ordering providers you select as your partner.

Conclusion

It will cost you less to comply with the PCI DSS requirements than to take the risk of a data breach. The after math of the breach will cost time and money that no one wants to incur.