



### Does your business accept debit and credit cards as forms of payment from customers?

If you said yes, then your business could be at risk of a costly data breach. Just one data loss incident could cost thousands of dollars in fines and restitution, damage your business reputation, and restrict your ability to accept debit and credit payments. It could even put you out of business.

### What happens if I am not compliant with PCI and my customers' credit card data is stolen?

According to Visa and MasterCard, the cost of a violation leading to a data breach can range anywhere from \$5,000 to as much as \$50,000. Is this a price your business can afford to pay?

Lodi Beer, a microbrewery and restaurant in California, has felt the pain of not properly safeguarding customers' credit card information. The company unknowingly stored 11,728 credit card records in its point of sale system. PCI-DSS specifically states that track data from the credit card's magnetic strip cannot be stored. When data processed by Lodi Beer was breached, Visa and MasterCard fined Abanco, the restaurant's merchant account provider, \$27,000. Abanco then in turn passed that fine onto the restaurant. In addition to the fines, this small merchant has spent more than \$50,000 in remediation costs, legal fees, upgrades, etc. That is a huge amount of money for any small business.

#### KEY ADVANTAGES

- Affordable, Reliable and Simple PCI Compliance
- Automated network scans
- Vulnerability remediation support
- Assistance in completing the PCI Self-Assessment
- Turn-key policies and procedures
- Network configuration and support
- Affordable cost starting at just \$500 per year
- Optional Seal Program Available

#### PCI peace of mind from DeviceLogix

The DeviceLogix PCI Compliance Assistance Program includes network scanning, remediation assistance, procedural and technical support, self-assessment, and validation of your compliance status. The service is easy to use and designed specifically for level 3 and 4 merchants that need to successfully and confidently attain and maintain PCI certification.

#### When your business needs to ensure PCI compliance, turn to DeviceLogix

The Payment Card Industry Data Security Standard – PCI-DSS – is the payment card industry's response to the increasing number of credit card data thefts by hackers.

This industry standard mandates that all organizations that capture, process or store credit card information must demonstrate proof of compliance to the standard. The DeviceLogix PCI Compliance Assistance Program provides both turn-key and step-by-step guidance so that you can successfully navigate the PCI-DSS requirements.

#### Use DeviceLogix to make PCI compliance easier, faster and cost effective

The DeviceLogix turn-key approach allows you to focus on running your business while our team of experts assesses your organization, develops the required procedures for your unique environment, configures your network, and performs the required quarterly network scan. With DeviceLogix, you have a choice of how to demonstrate your compliance with PCI-DSS requirements based on how your organization processes credit card transactions.

The DeviceLogix PCI Compliance Assistance Program starts at \$500 per year. This includes unlimited scanning of one IP address. We designed our full-service PCI Certification Service for organizations with less than six million payment card transactions per year (PCI Levels 3 and 4).

### **Who has to comply?**

All merchants that store, process or transmit cardholder data, are required to comply with PCI-DSS – regardless of their transaction volumes. This applies to organizations of all sizes; in fact, experts say that hackers are increasingly targeting small business websites for information because these thieves realize that small businesses don't have the same security safeguards as larger companies. PCI-DSS compliance is serious business and failure to comply could result in substantial fines and penalties and could negatively impact an organization's reputation and customer loyalty.

### **What do I need to do to meet the PCI-DSS standards?**

Ensuring you meet the PCI standard comprises two basic steps:

1. Pass quarterly remote vulnerability scans conducted by a Visa and MasterCard "Qualified Independent Scan Vendor." Scans are required for all Internet connection points whether they are office networks or home/office connections (dial-up, DSL, cable or wireless) or permanent Internet servers such as your website and email server, etc.
2. Successful completion of a security self-assessment questionnaire. The self-assessment questionnaire asks specific questions about your internal security practices, both on your website and in your office.

### **What are my validation requirements?**

Level 3 and 4 merchants are required to complete a self-assessment questionnaire annually and conduct a quarterly network scan.

### **What are the common reasons for non-compliance?**

- Storing data that should not be kept at all
- Not adequately protecting processed or stored data
- Not regularly testing systems and processes
- Not assigning a unique ID to each person with computer access
- Lack of tracking and monitoring of access to computing resources and credit card data
- Not installing and maintaining a firewall to protect credit card data
- Using vendor supplied "default passwords"
- Not having appropriate procedures to address information security
- Not restricting access to credit card data
- Not developing and maintaining secure systems and processes
- Not encrypting credit card data across public networks

### **How much does it cost to become PCI compliant?**

"It may cost you very little to become compliant. Let DeviceLogix evaluate your current stance and help you build a plan from there."

**Please visit our website at [www.device-logix.com/pci](http://www.device-logix.com/pci) for more information**