Practices for Protecting Credit Card Data

If you accept credit card payments, you are required to comply with some level of Payment Card Industry Data Security Standards (PCI DSS or more commonly called PCI), a set of requirements designed to ensure that any company that processes, stores and/or transmits credit card data maintains a secure environment. Failure to comply can mean the loss of your Merchant Account—the contract which gives you the approval to accept major credit cards (VISA, MasterCard, Discover, American Express, JCB), a fine and open your organization up for liability charges.

DEFINITION

Credit card data includes the full primary account number (PAN) or the full PAN and cardholder name, expiration date and/or service code.

PSN Takes on the Burden

Since PSN processes, stores and transmits credit card data on your behalf, we are required, and do maintain, a Level 1 PCI Certification. PSN also only provides credit card terminals which are compliant with PCI—no credit card data is stored in the machine; all data is transmitted according to PCI protocols to the PSN system.

Your Responsibilities

It is important to understand that if your staff writes down a credit card number from a customer who calls in, your organization allows customers to write their credit card numbers on bills and return them to your office or if you have customers fill out authorization forms for setting up recurring payments, for examples, you are responsible for proper handling of that data.

Procedures Your Organization Must Follow

If you are in possession of customer credit card data, you must follow these procedures:

1. If you must maintain the document with credit card info (such as an authorization form): Use a Sharpie-type marker to fully cover all but the last four digits of the credit card number. Also, fully cover the credit card number on the back side of the document (the show-through). You must then keep the document in a secure location—under "lock and key"—with monitored access.
2. If you do not need to maintain the document: Use a cross-cut paper shredder.
3. Depending on your credit card volume and if you are accepting credit card payments in your office, you may be required to complete a self-assessment questionnaire. You would receive the questionnaire via email. Please fill it out promptly.

RECOMMENDATIONS

We highly recommend that whenever possible you follow these practices:

1. Never have customers write credit card numbers on bills or other forms.
2. Never allow staff to write credit card numbers down; instead, they should be entered directly into the PSN system.
3. If you are accepting recurring payments by credit card and if the customer cannot go online to PSN, have the customer come to the office to provide the information. Have them fill out an authorization form but only write down the last four-digits of the credit card number. Your customer can tell your staff the full credit card number which is entered directly into PSN—the full card number is never written down.
4. Make sure all previously stored credit card data has been removed from your computer systems or other digital media.
5. You should follow these same practices for customers' bank account information, as well.

PSN Payment Service Network, Inc.

www.PaymentServiceNetwork.com • 866-917-7368
2901 International Lane, Madison Wisconsin 53704