Article published on December 3rd 2011 | Business

If you run an online business, accepting customer payments through all major credit cards and e-checks is very much essential these days. Even so, when merchants determine to accept payments online, they should also consider the potential risk of credit card fraud. The findings of various researches have revealed that traditional as well online businesses have incurred billions of losses in fraudulent transactions. Luckily, the modern technologies offer proven techniques for successful fraud management and prevention.

Address Verification Service or AVS is an uncomplicated technique that reduces your probabilities of accepting payment through a stolen credit card. At the time of processing an online credit card transaction, you need to ensure that the billing address and zip code of the card holder are captured. As soon as you capture these details, you are all set to process the sale. You point of sale (POS) system will check AVS with the card issuing bank. In case you don have an AVS mismatch, you must take steps not to accept the transaction. So, executing AVS can definitely be effective in preventing credit card fraud.

Card Verification Value (CVV/CVV2) is identical to Address Verification Service. You can detect CVV which is usually a 3-digit code on the backside of a credit card. Similar to AVS, CVV is inserted at the point of sale and then matched with the CVV of the card issuing bank. In case of a mismatch, you must proceed to decline the transaction. For highly efficient fraud management, web-based merchants should make CVV a mandatory field when customers fill out the online transaction form.

More sophisticated fraud protection services give merchants the ability to block transactions in terms of Internet Protocol (IP) address, country of origin and other parameters to filter out frauds. These services can be availed from online payment processing companies as supplementary ones.

Merchants who need to store the credit card details of a customer must make use of a data storage service complied with PCI DSS. Such a service permits businesses to transfer and store the payment details of the customer in a Level 1 PCI compliant data center. As soon as the customer data has been safely transferred and stored, the merchant can subsequently kick off transactions remotely with no need to retrieve credit card or e-check data directly. This fraud management process is completed without storing the payment details of the customer in the merchantâ€™s local database or payment program.

Another way to prevent credit card fraud is reviewing and executing the Payment Card Industry Data Security Standard (PCI DSS) policies. Business owners can reexamine PCI DSS policies over the internet. If youâ€™re already using a PCI certified POS solution and donâ€™t store payment informatio locally, youâ€™re performing exceptionally well. Nevertheless, merchants must get in touch with their merchant account provider for further information.

Article Source:
http://www.articleside.com/business-articles/online-credit-card-fraud-management-tips-for-merchants.htm - Article Side

Anthony Taylor - About Author:

Anthony Taylor is an expert in Internet security issues and has been associated with AlgoCharge, which is one of the leading online merchant services to prevent a credit card fraud. The company offers an integrated solution to payment processing and a fraud management using advanced algorithms.

Article Keywords:
fraud management, credit card fraud

You can find more free articles on Article Side. Sign up today and share your knowledge to the community! It is completely FREE!