

Merchant Requirements for Securing Cardholder Information

Your business and company reputation is at stake if you do not treat your customers data with the care it deserves.

For many customers, the payment by credit or debit card is an important part of their life as it is convenient and often the only way to pay for goods and services. Businesses that don't keep the cardholder information secure run the risk that customers go elsewhere for their purchases.

An increasing number of account compromise cases which appear regularly and more frequently in the media is alarming as it shows that more and more fraudsters are searching for ways to prey on consumers for fast money, and careless businesses make it easy for the criminals to do so. Businesses which do not keep company and customer information safe expose their vulnerability to fraudsters, and open themselves up to legal actions when crime does occur.

The concern is more pressing now given the sharp growth in the number of online merchants and transactions. Being compliant with international standards is now made simple and within reach. The payment brands have compiled a checklist to make it easy for you to see how well you secure your business information, or what you need to do to meet the minimum standard.

If you have any questions or would like to have more information, please visit our websites or contact your representatives for any of the card brands sponsoring this correspondence.



*Diners Club
International*



www.mastercard.com



www.visa-asia.com/secured

Basic Guidelines

Do not store sensitive cardholder information

- Do not store the following after authorization
 - Full contents of track data from the magnetic stripe of the card
 - Card validation Code: the three-digit value printed on the signature panel of a mastercard, VISA, JCB or Diners Club card and the four-digit code printed on the front of an American Express Card.
- Store only the customer's account information that is necessary for your business and only with the cardholders knowledge and approval (e.g. name, address or email address)
- Store all data containing cardholder information (e.g. authorization logs, transaction reports and transaction receipts) in secure place that allows access to authorized personnel only
- Encrypt account numbers on receipts and in databases or use only a part of the account number (e.g. print the first 6 or last few digits of the account number on receipts)

Destroy cardholder information after use

- Securely destroy all media containing transaction data with cardholder information that is no longer needed for business reasons.

Use only secure agents or third parties

- Advise your acquiring institution or processing contact for each card brand of any agents that you engage in the processing or storage of transaction data. (Agents include vendors, processors, software providers, payment gateways or other service providers.)
- Use only agents that meet all card scheme security requirements for the protection of cardholder data. A list of these compliant entities is available on the card schemes websites. Any violation by your agent may cause unnecessary financial exposure and inconvenience to your business.

Report all security incidents

- Immediately notify your acquiring bank or processing contact for each card brand if transaction data is accessed or retrieved by any unauthorized entity.
- Have systems and procedures in place to stop the unauthorized usage of compromised data immediately. Such incident response procedures will not only protect your customers in the most responsible manner, but also minimize yours and others financial losses.

