PCI DSS

What is PCI DSS?

Payment Card Industry Data Security Standard (PCI DSS) presents international rules defining conditions for treating cardholder data contained in payment cards. Fulfilments of these international rules are required by card associations, and are aimed at organizations processing, transmitting and storing cardholder data (from payment cards and card transactions). The purpose of such international rules is to reduce risks of data breach and its subsequent misuse. Standard PCI DSS as a model framework for insuring security contains best practices to minimalize risks of data stealing.

Protection of cardholder data contained in payment cards poses a real problem worldwide. Data protection must be dealt with not only by banks issuing payment cards but also by merchants accepting them. Obviously, payment card data must be protected by cardholders themselves.

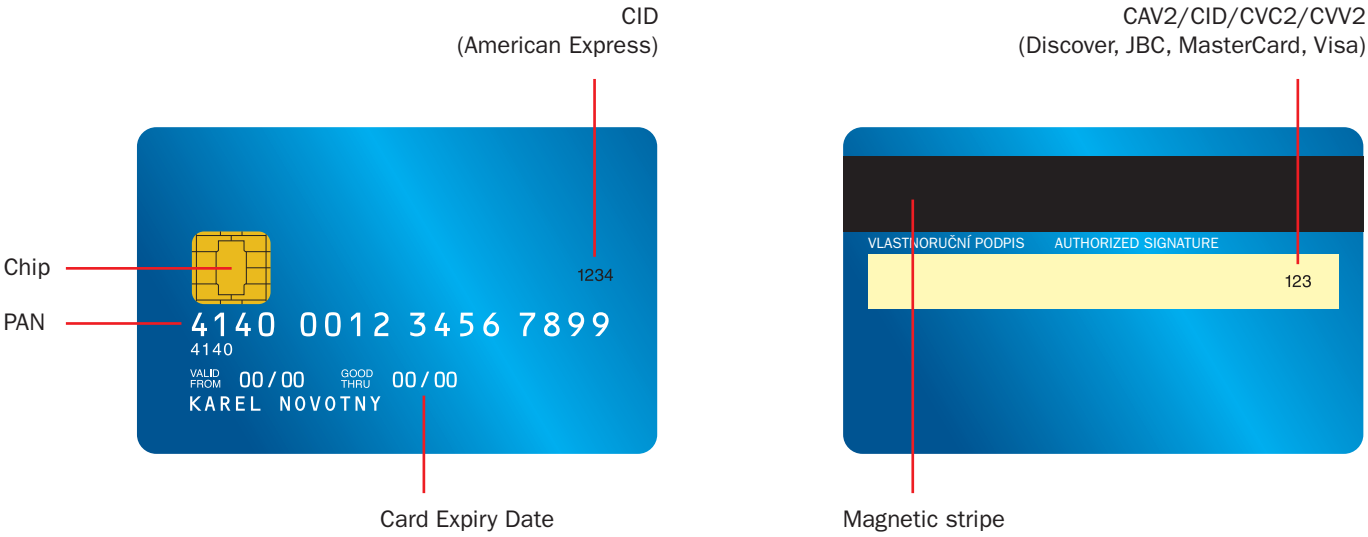
If you accept payment cards, whether you are a large international company or an owner of a single store, whether you run a retail shop or an internet shop, it is vital that your business activities must be in compliance with PCI DSS security standards.

Compliance with PCI DSS international rules is obligatory for all merchants accepting payment cards and it is strictly and without distinction required by all banks around the world.

As a merchant, you are responsible for cardholder data protection, particularly at the point of sale, and for its secure transmission into a payment system. It is your responsibility to set up and secure systems you are using, so that data of your clients are not endangered, including systems of your partners and vendors. The best practice how to minimize possibility of data breach is not to store **any card data at all**.

What card data should be protected?

a) Cardholder data contained in payment cards – card number, expiration date, name of the cardholder. If it is inevitably necessary, these data can be stored under maintaining security requirements following from the PCI DSS standard.
b) Sensitive Authentication Data (i.e. codes CAV2/CVC2/CVV2/CID, full magnetic stripe data, personal identification number (PIN)). **Storing of this data is not permitted under any circumstances!**



Sensitive data can be stolen from several places:

– Payment terminal
– Space, where paper receipts containing such data are stored
– Computer system
– Recordings from hidden camera
– Secret recordings from cable or wireless connection of your company

Offenders currently concentrate on small businesses whose systems are often less resistant against assault and therefore are easier sources of card information. Also for this reason the compliance with PCI DSS standards is obligatory for all merchants accepting payment cards.

Why is PCI DSS compliance so important?

– Your system is secure and payment card cardholders can trust you. Customer confidence increases probability that they will return to you and will recommend your company to others.
– Improving cooperation with acquiring bank and other subjects – partners, whom you need for your business.
– Diminishing the risk of extraordinary financial expenditures (for example as a consequence of card data misuse for fraud and other criminal activity).
– Reduction of costs for possible investigation and legal representation.
– Reduction of risks from negative media interests in your company.

What are consequences of not meeting PCI DSS reguirements?

– Unfair handling of payment card data can have negative effect on all interested parties – customers, merchants and financial institutions.
– One single incident can cause damage to your reputation and problems in your business.
– As the ultimate consequence your company could be sanctioned, and you could be required to indemnify costs related to investigation of data misuse and related legal actions.

How can we help you?

Your acquiring bank shall upon your request inform you into what level of categorization you belong according to your number of transactions and what criteria apply to your category for verification of PCI DSS international rules.

Any necessary information concerning security requirements in the area of payment cards acceptance, including the PCI DSS standard, categorization of subjects and corresponding obligations, is available at **www.pcisecuritystandard.org**.

Thank you for your engagement in payment cards data protection.