

Payment Card Industry (PCI) Data Security Standard

To protect your business, your customers (cardholders), and the integrity of the payment system, the card industry has set in place a set of requirements governing the safekeeping of account information. This standard is known as the Payment Card Industry (PCI) Data Security Standard and is endorsed by all leading payment brands, among them

Visa, MasterCard and Diners Club.

Who does PCI apply to?

It is required that all entities that participate in the international payment systems i.e. those entities that process, store or transmit cardholder account and/or transaction information adhere to the requirements of the standard. This

includes merchants, processors, gateways and Payment service providers, and other third party service providers such as network providers, data consolidators, media back-up companies, and web hosting companies. We will contact you individually in order to discuss how the requirements applies to your company.

Summary of Card Company Requirements Governing Cardholder Information Security	
Storage of Cardholder Information	<ul style="list-style-type: none"> Do not store the following under any circumstances: <ul style="list-style-type: none"> Full contents of any track from the magnetic stripe on the back of the card. Card-validation code (CVV2/CVC2), the three-digit value printed on the signature panel of the card. Store all material containing this information (e.g., authorization logs, transaction reports, transaction receipts, car rental agreements, and carbons) in a secure area limited to authorized personnel. <p><i>Store only that portion of the customer's account information that is essential to your business—i.e. name, account number or expiration date.</i></p>
Destruction of Cardholder Information	<ul style="list-style-type: none"> Destroy or purge all media containing obsolete transaction data with cardholder information.
Use of Agents or Third Parties (Vendors, Processors, Software Providers, Payment Gateways, or Other Service Providers)	<ul style="list-style-type: none"> Advise us of any agents that engage in, or propose to engage in, the processing or storage of transaction data on your behalf regardless of the manner or duration of such activities. Make sure these agents adhere to all rules and regulations governing cardholder information security. Any violation by your agent may result in unnecessary financial exposure and inconvenience to your business.
Reporting a Security Incident	<ul style="list-style-type: none"> In the event that transaction data is accessed or retrieved by any unauthorized entity, notify Euroline immediately.