What is PCI?
PCI stands for Payment Card Industry.

The Payment Card Industry Security Standards Council is an industry body made up of organizations like Visa, MasterCard, American Express and Discover. The Council has agreed upon a single, common security standard that Merchants are required to meet.

The full name for this standard is the Payment Card Industry Data Security Standard (PCI DSS). Merchants must meet this set of security requirements if their business accepts, transmits or processes customer payment cards, such as credit cards or debit cards.

What is the PCI DSS?
PCI DSS stands for Payment Card Industry Data Security Standard.

This is a technical and broad-ranging set of security requirements created by the Payment Card Industry, laying out what Merchants need to do to protect customer information.

The PCI Council requires that Merchants meet this set of security requirements if their business accepts, transmits or processes customer payment cards, such as credit cards or debit cards.

All merchants that accept debit or credit card of the common card scheme organisations have to comply with the PCI DSS regulation and have to undergo the registration and / or certification according to their business.

Merchants that do not comply with these requirements can be penalized in a number of ways, up to and including having their card-processing privileges revoked, leaving them unable to accept customer payment cards.

What does a merchant have to do in order to satisfy the PCI requirements?
To satisfy the requirements of PCI, a Merchant must do two things:

1. Comply with the Data Security Standard by meeting all of the requirements laid out in the Data Security Standard, and
2. Validate their compliance. This means the Merchant must SHOW (in a manner appropriate to their size and situation) that they are complying with the Data Security Standard.

For some Merchants, such as those with a high volume of card transactions, or with a history of security problems, validation involves on-site audits by certified professionals, but for many Merchants the primary requirements are:
   - Annual completion and submission by the merchant of a PCI Self-Assessment Questionnaire (the SAQ); and
   - Where appropriate, undertaking a quarterly network vulnerability scan by a certified scanning company.

What is the PCI Self-Assessment Questionnaire or SAQ?

The Self-Assessment Questionnaire (SAQ) is a form that Merchants may be required to complete every year and submit to their Acquiring Bank. It was created by the PCI Council. Completing a Self-Assessment Questionnaire helps Merchants do two things:

- Check their Compliance, by finding out for themselves if they are in compliance with the Data Security Standard
- Complete part of their Validation

Merchants now need to identify which of the Validation Type categories they fit into, and then complete the appropriate Self-Assessment Questionnaire for their category.

For some Merchants, the appropriate Self-Assessment Questionnaire is short and simple, while for other Merchants the appropriate Self-Assessment Questionnaire is long and extremely technical. Note that for all versions of the Self-Assessment Questionnaire, Merchants will only be considered compliant if they pass (or can answer “Not Applicable”) to ALL of the questions in the Questionnaire.
What is meant by Compliance?
Being “Compliant” means that the Merchant meets all of the requirements laid out in the Payment Card Industry Data Security Standard. The requirements for Compliance are the same for ALL Merchants, large or small. However, smaller Merchants typically avoid many of the Compliance problems that larger organizations face, because their systems and networks are usually simpler.

What is meant by Validation?
Validation means that a Merchant can demonstrate, via standard documents and/or tests, that they are meeting the PCI DSS requirements. Different Merchant types face different Validation requirements, depending on which of four levels they are assigned to.

Is PCI a government program or law?
No, PCI is not, in itself, a law. The standard was put together by business organizations including Visa, Mastercard and the other major card companies. Merchants that do not comply with PCI DSS are not necessarily breaking any law, but they are probably violating their Terms of Service or contract with their acquiring bank and the card associations. This means that the Merchant might be penalized or sued, or these companies might refuse to work with the Merchant. This means that the merchant would be unable to process credit or debit cards.

What is a network vulnerability scan?
While not all businesses will require scans, if one is needed, a vulnerability scan is an automated, non-intrusive process that assesses the Merchant’s network and web applications from the Internet (on the external-facing IPs). The scan will identify any vulnerabilities or gaps that may allow an unauthorized or malicious user to gain access to the network and potentially compromise cardholder data.

What Happens If I Don’t Become PCI Compliant?
If your business fails to become PCI compliant\(^1\), you could be putting your business at greater risk from the growing threat of payment card data breaches and theft, which may result in substantial penalties (such as fines from banks, regulatory agencies, and card associations), fraud and charge backs, as well as legal costs and lost customers. If you fail to become PCI DSS compliant or to report your PCI DSS-compliant status with a third-party vendor to First Data, you may also be charged a monthly non-receipt of PCI Validation fee by First Data until such time as you become PCI DSS-compliant or report your PCI DSS-compliant status to First Data.

If your business experiences a data security breach, you could even lose your ability to process credit card payments. Perhaps more importantly, you risk the loss of customers.

How can I achieve PCI Compliance and Validation?
The First Data solution is an easy-to-use online tool that can help you achieve and maintain PCI DSS compliance more quickly and easily. It offers:

- **Step-by-step guidance to complete the annual self-assessment questionnaire (SAQ):** Our step-by-step application will direct you to the PCI SAQ that is appropriate for your business. You can complete the SAQ with guided support, ensuring each question is answered accurately.

- **Fewer questions to answer – in some cases, 85% fewer questions:** With "pre-SAQ" questions, we can pre-populate the appropriate SAQ answers – which are often the most difficult - minimizing the number of questions you have to deal with and speeding up the SAQ completion process.\(^1\)

- **Comprehensive support that ensures your questions get answered:** Have a question? With our built-in help, guides and security expertise, we can answer any PCI questions you may have – online and via chat, email and phone.

Are there additional fees to use the First Data solution?
An annual charge of €25.95 per MID on the portal includes your annual PCI self-assessment questionnaire (SAQ) and quarterly scans, if needed.

If you fail to become PCI DSS compliant or to report your PCI DSS-compliant status with a third-party vendor and not to First Data, you may also be charged a monthly non-receipt of PCI Validation fee until such time as you become PCI-DSS compliant or report your PCI DSS-compliant status to First Data. Please refer to our price list.

**Do I have to use the First Data PCI solution?**

Our solution is an on-line, automated self-assessment tool offered by First Data to guide our merchants through the PCI DSS compliance validation assessment process. It offers the support of a live help desk, provides information on potential vulnerabilities along with innovative security enhancements that may further protect our merchants' processing environments.

The benefits of using the First Data solution is that we can offer help/support which includes a guided, step-by-step SAQ tool help to complete the annual questionnaire with ease, an integrated scanning tool for merchants that are required to pass quarterly scan (if applicable) and comprehensive support online and via chat, email and phone to ensure your questions get answered.

We have developed the solution in conjunction with a QSA to make the self-assessment validation process for Level 3 and 4 merchants much simpler for merchants to complete. In addition, an Approved Scanning Vendor (ASV) is used to support quarterly network scans required for merchants processing payments over the internet.

For merchants using terminals provided by First Data or TeleCash we are able to offer a shortened process in case the merchants business is not T&E, gambling and other high risk business.

For PCI Level 1 and 2 merchants that require a QSA for their PCI DSS compliance validation, a PCI Approved QSA can be found on the PCI SSC’s website. We can also supply one at a reduced cost. Please ask for more details. Price is based on merchant complexity.