globalpayments

PCI Frequently Asked Questions

What is PCI DSS?
The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements which all companies that process, store, or transmit card information need to follow, to maintain a secure environment.

Why is it important to achieve compliance?
It's important because by achieving compliance you avoid a potential data breach and the loss of your customers' data. Even a small breach typically costs thousands of pounds as you'll need to fix the data leak, pay for a forensic investigation and may also face Card Brands penalties. This can have a huge impact on cash flow and staff resources, and sadly we know of some companies that have ceased trading following a data breach.

What is a PCI Non-Compliance Fee?
PCI non-compliance fees are charges incurred when you don't attest that you are PCI DSS compliant to your acquirer.

Why didn't I receive any reminders about my PCI compliance?
After you've taken your first transaction, a letter is sent to your trading address which explains what is needed, the deadlines and the fees that apply if you fail to meet the deadline.

You'll also receive annual renewals. These are emails sent out by SecurityMetrics on a weekly basis about four weeks before the expiry date. You'll also receive a letter from us, which is sent to your trading address one month before the expiry date.

Why haven't I been informed about PCI DSS and the penalties of not being compliant?
In the question above, we outline when letters for both new merchants and those due to renew their compliance are sent to the trading address. In these letters we explain the details, including the fees for not being compliant. They are also explained in the Terms of Service and Know the Risks documents.

How are the PCI Non-Compliance Fees calculated?
PCI non-compliance fees are charged one month in arrears and calculated at either 15 pence per transaction or £75 - whichever is greater.

How often do I need to complete my PCI compliance?
Self-Assessment Questionnaire (SAQ) Only - you need to complete an SAQ annually.
SAQ & Approved Scanning Vendor (ASV) Scans - as well as completing an SAQ, you may also need to have quarterly network scans if you have internet-facing internet protocol (IP) addresses. Network scans help identify vulnerabilities and misconfigurations of web sites, applications, and information technology infrastructures with Internet-facing IP addresses. However this should be done automatically by your ASV provider and sent to you, with the results.

Do I still need to pay PCI Non-Compliance Fees if I only missed the deadline by a few days?
Yes, your compliance status is taken on the last day of the month, this means if you miss that deadline by a few days you have still been non-compliant for the entire month and non-compliance fees will apply.

Will the PCI Non-Compliance fee be refunded once compliance is achieved?
No, the fee is charged for a period of non-compliance. By becoming compliant, you will stop future charges being applied.

I have already achieved compliance, why am I still being charged?
Non-compliance fees are charged in arrears. For example, if you were non-compliant on 31st May, you'll see the fee associated with this period on your July invoice which you receive in August.

Will I still be charged PCI Non-Compliance Fees even though I've been closed throughout the COVID-19 pandemic?
Yes, PCI non-compliance fees will still be charged. If you're unable to pay or feel this is unfair then you should contact either your relationship manager or the helpdesk.

Do other Acquirers charge PCI Non-Compliance Fee?
Yes, other acquirers do charge fees for PCI non-compliance.

Is the Non Secure Fee the same as PCI Non-Compliance Fee?
No, they are not the same. A Non Secure Fee is applied to transactions that aren't taken using Chip & PIN or 3D Secure online. These transactions carry an additional risk and are more likely to be susceptible to fraudulent activities. To minimise this cost, where possible ensure that you process transactions securely.

What is a secure transaction?
A transaction that has been processed with additional cardholder verification such as Chip & PIN or 3D Secure.

Issued 01/2021