PCI Powered by SOTpay

SOTpay™

Looking for an easy and cost effective way of securing your telephone payment environment?

Looking to eliminate fraud related chargebacks, reducing costs and delivering a great customer experience, in a PCI DSS compliant manner?

You're in luck. PCI Powered by SOTpay™ allows you to handle 'Card Not Present' telephone transactions securely, by sending your customer secure SMS and email hyperlinks helping to combat fraud, reducing the scope of PCI DSS compliance and delivering a great customer experience by allowing your staff to maintain voice contact with your customer during the whole transaction.

It even allows you to deliver to a third party address without risk and in many cases reduces payment processing charges from your acquirer.

Why Your Customers Will Love It

In our experience, consumers do not like disclosing their sensitive card numbers to a stranger over the telephone, as it increases the risk of data compromise. PCI Powered by SOTpay™ allows customers to manually input their card information in a secure environment, as opposed to reading out their sensitive data over the telephone. Your customers can access the payment arena via SMS or a secure email hyperlink and complete the transaction in a few simple clicks.

Key Benefits

PCI DSS compliant 'Card Not Present' Telephone Payment Solution;

Mitigate the risk of fraudulent card data being used in CNP telephone order payments, by sending secure SMS and email hyperlinks which facilitates additional cardholder authentication, eliminating fraud related chargebacks. This saves valuable time and money with complex PCI DSS requirements.

Take Care of PCI;

Take care of complex PCI DSS requirements, by removing the sensitive card data from the merchant's sales environment to reduce the burden of PCI compliance.*

Third Party Delivery Solution;

Accept more transactions and improve the customer experience by being able to deliver to an alternative address from the registered billing address, without liability.

PCI Powered by SOTpay

SOTpay

The system also uses an ID authentication system to help ensure that only the genuine cardholder can process the transaction, mitigating the risk of chargebacks related to fraud.

Why You Will Love It

According to the UK Finance, around 550 million CNP MOTO transactions are processed annually in the UK which equate to £65bn in sales. Can your business really afford not to accept secure CNP MOTO transactions?

This solution removes all sensitive card data from the merchant environment. This allows the consumer to safely input their card details without sharing personal payment card information with the telephone agent, thus removing the environment from the scope of PCI DSS. With UK compromised card fraud levels reaching £618m in 2016, it is more important than ever for businesses to protect themselves from fraudulent telephone transactions. The application authenticates the identity of the cardholder, thus mitigating the risk of an order being paid for using fraudulent card data. Because transactions are 'secured' through authentication this often leads to reduced processing charges from the acquirer. It also means goods can be delivered to third party addresses, without the risk of fraud related chargebacks, saving you both time and money.

PCI DSS COMPLIANT

2018 UKCCF AWARDS WINNER

Key Benefits

Reduce Processing Costs;

It has already saved merchants thousands of pounds in processing fees, as our transactions are deemed as 'secure' by many acquirers and therefore processed at a beneficial rate.

Fast Deployment;

The application does not require integration with your existing telephony infrastructure or any additional hardware, so deployment can be swift. The cloud based solution is therefore a cost effective alternative to unattended IVR and attended DTMF technologies.

* Please note. Whilst the application reduces the scope of PCI DSS within the telephone sales environment, it does not eliminate the need for the merchant to meet their obligations under PCI DSS Requirement 12, relating to the management of Third Party Service Providers and having an Incident Response Plan.