The Simple Guide To Taking Payments Online

In simple terms, the process of taking credit and debit card payments on line follows this process:

1. Customer visits your site

2. Customer clicks on a "buy item" button or select to purchase items within your purchasing pages

3. The selection is added to their shopping cart, if you have one, or is included in a transaction summary, ready to complete the transaction through payment.

4. Once at the 'checkout', the customer's personal and financial details are recorded via a secure form.

5. Details submitted on the form are transmitted to a payment gateway service, which is separate from the shopping cart. The gateway service securely routes the information through the relevant financial networks to gain authorisation.

6. If the transaction is successful, the customer's credit card account is debited and your merchant account is credited.

7. Once all funds have cleared, you are then able to transfer the money to your ordinary business bank account.

Getting Started

Before you can start accepting payments online there are a number of decisions you will need to make and some actions you must undertake. Broadly speaking they are (in order);

-

If you want a quick overview of the key steps to being able to take online payments click here

Internet Merchant Account– Before you can start accepting Credit and Debit cards online you'll need to get an internet merchant account, this will allow you to accept and hold payments from credit card transactions. An Internet merchant account is very similar to the merchant accounts used for mail order and telephone orders, because the cardholder is not present in both cases, these are referred to as CNP (cardholder not present) transactions. Most high street banks in the UK offer Internet merchant accounts, but can be quite selective, sometimes preferring business and store owners to have a proven track record of at least two years trading. There are also specialist companies offering merchant accounts. Click here for more information and links

A Payment Service Provider (PSP), such as SECPay, is a payment gateway. It is a separate service to that of the acquiring banks, and acts as an intermediary between the merchant's website or shopping cart and all the financial networks involved with the transaction, including the customer's credit card issuer and your merchant account. The payment gateway checks for card validity; encrypts the transaction and card details; ensures they are sent to the correct destination; and then decrypts the responses, which are returned back to your website or shopping cart either as an authorisation, referral or declined transaction.

This is a seamless process and your customer does not directly interact with the gateway, since data is forwarded to the gateway via your shopping cart or online payment page through a

secure (SSL) connection. By using SECPay your website is configured to send information in a format that is acceptable to each particular gateway.

Whilst we of course want you to choose SECPay to handle your payment processing requirements, we recognise that most merchants will want to consider a few alternative suppliers. To help you, we've broken down the key industry terms and offerings so that you can compare openly and fairly to make the right decision for your business.

Key Industry Terms

Interface – This refers to the technology and code that is used to integrate your website with the services of the payment processing supplier (who in turn interfaces with the banking systems). Ideally you want a supplier that offers a full range of interfaces from a simple payment page through to XMLRPC VPN.

Set-up Costs – Most Payment Service Providers (PSP's) charge a set-up fee for new accounts, these can range from £50 [SECPay] to £250 (excluding VAT).

Transaction Charges – This is the cost per transaction processed, which is in addition to set-up charges and monthly service charges. Some PSP's charge a percentage of the transaction with a minimum charge. This inevitably ends up a more expensive option as the minimum cost is incurred on low value transactions, and the percentage on all others. Some PSP's charge for "Blocks" of transaction. These can appear to be at a lower cost per transaction but if you do not use the entire block, in most instances you'll end up paying more. With SECPay you only pay for what you use.

Monthly Service Charges – Most PSP's charge a monthly standing charge, that can range from £10 through to many thousands. Monthly service charges and transactional charges are always linked. In most instances the higher the volume, the lower the transactional rate and the higher the service charge.

Service Availability – This is a key consideration for all online merchants as you will not be able to take payments when the payment service is unavailable. All systems are periodically taken off-line for development and upgrades: the key point for comparison is what is the guaranteed service level and what is the actual performance. For SECPay, the guaranteed availability standard is 98.5% per month, and the achievement is currently 99.7% (rolling for the last 12 months).

Virtual Terminal – This is a terminal interface that you, as a merchant, can access via secure log-in. The virtual terminal enables you to process mail and telephone orders and make refunds. Most PSP's will charge extra for virtual terminals: with SECPay it is part of the overall package, and is included in the monthly service charge.

Funds Clearance – This refers to the time between when the transaction is authorised and when the funds are credited to your merchant account and available for use. For many of the Payment Services offered by the key high street banks this can be as long as three weeks. With SECPay it is between 48 and 72 hours from transaction.

Chargeback – these refer to transactions that, whilst being made on a valid credit card, are disputed by the cardholder. Unless you have gained secure verification from the cardholder, the transaction value will be debited from your merchant account by the acquiring bank. Before choosing your PSP make sure they offer all the currently available anti-fraud screening choices, such as CV2, AVS and 3D secure (also known as verified by Visa and Mastercard Securecode).

Accredited Standards - finally, it is always advisable to choose suppliers that have achieved internationally recognised standards of security and that meet industry wide quality accreditation standards. SECPay is the only independent PSP to achieve the coveted ISO 9001 quality

standard.

The Payment Service Provider Checklist
What security verification and anti-fraud measures are available?
What interfaces are available and are they all Secure Socket Layer (SSL) based?
What are the set-up, monthly service and transactional charges?
What is the cost of a Virtual Terminal?
What is the service availability performance for the past 12 months?
How long does it take for the funds to be cleared into your merchant account?
What security and quality standards are they accredited with?
What payment gateway integration options do they offer and are these compatible with your needs (or those of your web-developer?

SECPay's Answers to PSP Checklist

The Customer's Perspective

After deciding on items to purchase on your website, the customer wants to conclude the transaction as simply and easily as possible. Entering their details is a chore and they certainly don't want to have to navigate multiple screens to pick a credit cards and enter billing address information. Customer's certainly don't want to feel like they've been re-routed and ended up somewhere else for the payment processing, in most instances they want to be taken to a secure checkout page where their order can be reviewed and card details can be entered. At this stage the Web Site should switch to the Secure Socket Layer (SSL) mode. SSL is a widely used encryption technology which means that the information passed back and forth between the checkout page and the server is encrypted thus helping to prevent the credit card information from being stolen. For customers using most up to date releases of Internet Explorer a padlock symbol will appear on their browser to show and reassure them, that the page is secure. SECPay offers SSL encryption and protection on all their interfaces to ensure that both customers and merchants are protected to the best industry standards.

Customer Perspective Checklist
How many screens must be entered before the payment can be processed?
Is the security fully verified Secure Socket layer?
Does the payment page feel integral to the website?
What happens to the transaction if the customer clicks on the back button after they confirm purchase?

SECPay's Answers to Customer Checklist

Integrating the payment gateway with your site

At its simplest level, a payment page from a payment services provider (such as SECPage from SECPay) works using HTML forms submitted over SSL. A secure server at your end is not necessary but can be used if you wish. The lifecycle of a typical transaction processed through SECPage consists of four steps:

-

In-Process

Authorisation* – Merchants must obtain authorisation in order to charge the credit or debit card for the goods ordered. In most cases, authorisation, is simply a check to see if the card has been

reported stolen and that there are sufficient funds available. This is done seamlessly within the transaction handling done by SECPay. Currently there are two ways in which an authorisation can be sought:

-

***It is worth highlighting that Authorisation and processing is performed by the acquiring bank and is not a guarantee of payment.**

Capture

Once authorisation is achieved, the credit card or debit card is debited. This tends to happen automatically at the same time as authorisation, providing that the merchant guarantees that the order will be delivered within an agreed time period. If this is not the case, capture should take place when the order is ready for delivery, and will require a manual transaction completion process.

Address Verification

The Address Verification System (AVS) AVS decreases the incidence of accepting fraudulent transactions by verifying the cardholder's billing address with the card issuer. Implementing AVS on your transactions may also benefit you by resulting in lower transactional fees charged by your Merchant Bank.

Fraud Prevention

Online Fraud is a reality, and whilst it is a very small percentage of overall transaction conducted over the internet (less than 1%), it is nevertheless a key business risk and one that you should take seriously. SECPay provide a range of fraud detection and prevention tools, and is rapidly expanding these to ensure that we remain amongst the best in our field in identifying possible fraud and helping our merchants make informed choices about which transactions to reject.

Who carries the risk

Unfortunately, in most instances the retailer (merchant) carries a good proportion of the risks associated with potential Fraud. The primary risks are associated with lost and stolen cards, should you accept one without having verified the cardholder and sought authorisation from the acquiring bank, then you will receive a re-charge from the bank which will be for the full amount of the transaction, as well as an administration charge – these are referred to as chargebacks. This is, of course, in addition to the cost of the goods you've provided to the thief.

The first step in preventing fraud is to identify potentially fraudulent transactions. SECPay allows you to set the parameters of transaction acceptance. In broad terms when a cardholder name and UK billing address matches the UK delivery address, and the CV2 code is verified by the bank, and the bank authorises the transaction, then this is known as positive match transaction which carries a very low profile of risk. If however the billing address and delivery addresses are different, then this can increase the risk exposure. If the delivery address is overseas in countries which have a high incidence of fraudulent use of credit cards, then it's a good idea to place these transactions into a holding area for you to manually verify. It is this principle that is behind the Fraud management systems offered by SECPay. We allow our merchants to make decisions on the risks that are unique to their business. If you are a mail-order hamper supplier offering specialist hampers for Ex-Pat Britons living abroad, then a high percentage of your orders will have overseas delivery addresses (and potentially UK Billing Addresses), and may be perfectly legitimate transactions.

The important thing is to take informed decisions on transactions that have a higher risk profile than you are prepared to accept as the norm. When choosing a Payment Service Provider you should pay close attention to the breadth of their Fraud prevention and management tools as poor

tools will result in two impacts: firstly you will carry higher fraud losses than you need to, and secondly if the tool doesn't work with the latest development and fraud management data you'll end up rejecting transactions that are perfectly legitimate. For details on SECPay's SECGuard active fraud management system click here.

Integration Options

SECPay offer an extensive range of integration options, including;

SECPage The security and privacy of all card details are maintained by our high levels of encryption, and the transaction is authorised within seconds. All transactions are cleared through to your acquiring bank at the end of each day.

XMLRPC – This refers to the API (interface) used to connect your website to our servers. In this instance it is written in extensible mark-up language (XML) and is a simplified cross platform toolset enabling connectivity between the different systems.

SOAP - Simple Object Access Protocol is a lightweight XML-based communications protocol designed for the exchange of information in a platform-independent, distributed environment.

In addition to the interfaces by SECPay we also offer additional connectivity in the form of a VPN (Virtual Private Network) connection, but this is ostensibly for larger merchants and accounts.

The actual integration of our payment service within your website is undertaken by developers, if you would like the full technical specification for this click here.

Test Accounts

SECPay offer the facility of a test account: it is available before you set-up your SECPay account. The test account enables you to better understand how the SECPay system works. To access the test account click on this link

Testing your payment facility

Once you have integrated your website with the SECPay payment processing service (using one of the interfaces mentioned previously) you will be able to conduct test transactions using legitimate credit card details (which won't be processed, as your account isn't set-live). You can perform as many test transactions as you wish, using a mixture of both valid and invalid card data. This will help you understand how the authorisation process works, and how to start managing the potential risks for your business.

SECNet – The merchant extranet from SECPay.

Once you have set-up your account with SECPay, you will be able to access SECNet. Within this information rich area, you will find additional information and support for all SECPay services. Most importantly, SECNet contains the virtual terminal for your account.

Virtual Terminal

In order to process phone or mail orders or from other locations, all you need is a PC connected to the internet with a web browser, and you will be able to use the SECPay Virtual Terminal which provides all the processing functions of a physical POS terminal, but with added convenience.

Reporting

Within SECNet is the online reporting toolset from SECPay. The reporting toolset enables you to check on authorised, cleared and refused transactions.

SECGuard

SECGuard is SECPay's active fraud management toolset that enables you to make informed choices on which transactions to accept automatically, those which to reject automatically and those that you wish to manually assess before either rejecting or accepting. This multiple level of Fraud management systems puts some of the most sophisticated anti-fraud systems and information in the hands of SECPay merchants, through an intuitive and easy to use interface.

Setting your Account Live

Once you have completed the previous steps and are satisfied with the outcomes of your test transactions, all you need to do is e-mail us at **admin@secpay.com** for your account to go live. In order to set your account live we will need to arrange with your merchant account provider that your account becomes live within the banking system. Most merchant account providers will set your account live within a couple of days. At our end, once we receive notification from your merchant account provider that they have set it live at their end we will set you account live within our system within a few minutes. From that point you will be able to take online transactions automatically and conveniently at the lowest possible cost.

Sign-Up Now
Go direct to our registration page
Set Up Account;