Fraud Whitepaper

Everything you need to know about Online Fraud in 10 minutes or less

- Introduction to Fraud
- Know your Fraud tools
- Protect your data
- PCI DSS requirements
- 5 ways to reduce fraud
- Tokenised payments
- Security Policy

To a greater or lesser extent, fraud concerns almost everyone involved in e-business. With margins tight and competition fierce, the prospect of losing money to fraud haunts many businesses.

Cyber criminals are becoming ever more inventive and although systems are developed and employed to tackle online fraud, cyber-criminals will always work to find a loophole. Online fraud can take place through stolen cards and identity theft, but can also occur as a direct result of poor security on the part of the vendor. A website without proper security measures could allow a fraudster to obtain sensitive details. Even poor security within an office environment could up-scale a minor office break-in to a full data breach, resulting in genuine customer card numbers being compromised.

In this whitepaper, we'll give you a run down of the fraud screening tools available, payment card regulations to help you maintain secure systems and tips on how to mitigate fraudulent transactions.

Know your Fraud Tools

The first step towards reducing the risk of fraud is setting up the correct fraud screening tools on your account. Most payment service providers (PSP's) will be able to provide you with a basic level of fraud protection; however there are different levels of protection available.

- **AVS**
  AVS or Address verification System checks the numerics in the billing address of the card against the address at which the card is registered.
- **CV2**
  CV2 or Card Verification Code is the three/four-digit authentication code on the back of credit or debit cards.
- **3D Secure**
  3D Secure is similar to an online version of Chip and PIN, where instead of a PIN number, a user-generated password is required. It aims to reduce the possibility of fraudulent card use by authenticating the cardholder at the actual time of the transaction. Subsequently this reduces your exposure to disputed transactions and charge-backs of this type.
- **Bespoke Tools**
  Some PSP's work with a third party that runs secure background checks on card data supplied by many sources. For example, whether the card or delivery address has been used in previous fraudulent activities.

Fraud Screening tools vary in complexity and effectiveness and it is worth noting that any results you get are only ever as good as the information provided in the first place. The more detail you gather about a customer or a purchase and provide to your PSP or fraud screening company, the higher the effectiveness of the results.

With the Sage Pay system, the parameters of these tools can be easily adapted to fit the unique requirements of your business. For example, you can set different rules for differing monetary values, so that if you want to apply strict rules for transactions over £100 and less stringent rules for those under £5, you can.

Protect your data

Taking payments without proper security measures in place could allow a fraudster to obtain sensitive card details. The scale of repercussions can run from reputational damage, right through to unlimited fines, which could devastate your business.

The Payment Card Industry Security Standard (PCI DSS) is a set of requirements designed to ensure all companies that process, store or transmit card information, maintain a secure environment.

Although PCI DSS is not yet a legal requirement, that doesn't mean that businesses can avoid it. Every business processing payments needs to be compliant with these regulations as best practice and often obtaining (or retaining) a merchant account is dependent on PCI DSS certification.

The first thing a vendor will need to do is find out which level bracket their business falls into – these are dependent upon the number of credit/debit card transactions they process per year.

- **Level 1**
  The highest level, merchants processing over 6 million Visa transactions annually
- **Level 2**
  Merchants processing 1 million to 6 million Visa transactions annually
- **Level 3**
  Merchants processing 20,000 to 1 million Visa transactions annually
- **Level 4**
  The lowest level, merchants processing less than 20,000 Visa transactions annually

Each level is broken down further into 12 steps to follow, which emphasises the need for encryption, access controls and firewalls. How stringent these are depends on which level you will be required to reach - Level 4, for example, can be as easy as a simple self-assessment questionnaire.

PCI requirements in a nutshell

Build and maintain a Secure Network

Requirement 1: Install and maintain a firewall to protect cardholder data
Requirement 2: Make sure that if you receive any vendor-supplied passwords, you create your own password straight away

Protect Cardholder Data

Requirement 3: Protect stored cardholder data
Requirement 4: Encrypt all cardholder data if you are sending it across open, public networks

Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software
Requirement 6: Develop and maintain secure systems and applications

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need-to-know
Requirement 8: Assign a unique ID to each person with computer access
Requirement 9: Restrict physical access to cardholder data

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data
Requirement 11: Regularly test security systems and processes

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security

If your business is struggling to understand, let alone achieve PCI DSS compliance, you are not alone. Sage Pay's soon-to-be-published Business Benchmark Report reveals that 42% of businesses don't know whether they are PCI compliant and only 27% fully understand the need for compliance. Although the regulations look like hard work, many of the requirements are common sense and this is where a Qualified Security Assessor (QSA) or other information security professional can help.

The good news for many merchants is that they can reduce their PCI DSS requirements by avoiding the need to handle sensitive payment card data in the first place. Merchants are able to do this if they use a service provider with certified Level 1 compliance, such as Sage Pay, to collect, store and transmit card data on their behalf.

So, if you can limit your exposure to PCI, we'd recommend it.

5 ways to reduce fraud

1. Check the telephone number and delivery address against the billing address. Call the number to check that the area code matches. You can even go one further and look it up on Google Street View to check whether the building matches your expectation
2. Be wary of a low-cost transaction followed by several high-value ones. Fraudsters will often test the water with a small purchase before becoming more ambitious. They will also choose to strike during times of peak online activity so they can hide in the data and go unnoticed. Be extra vigilant around your busiest times.
3. Be extra cautious of 'high-risk' countries. This is especially relevant as more e-businesses than ever are expanding their reach.
4. Check the email address to make sure it's valid (you'll get a bounce-back if it isn't) and be more suspicious of free, temporary and anonymous email addresses.
5. If everything checks out but you're still suspicious, consider sending goods by registered post to ensure you get a signature and avoid non-delivery claims.

Remember, you can always choose to void the transaction.

Tokenised payments: The next step?

Tokenised payments are the natural next step for merchants looking to restrict their exposure to card data. As with redirection models, the cardholder data is collected by the e-payment provider; however once a card transaction is entered into that e-payment provider's system, a random string of numbers and letters (the token) is generated to correspond to each card and passed back to the merchant. This token can then be used as the merchant wishes, without the security concerns of card data getting into the wrong hands – even if it could be accessed, the token would be indecipherable.

In particular, this technology can facilitate a range of payment methods:

Delayed or deferred payments – to allow a merchant to take payment on delivery, but to collect and store the card details securely when the initial ordered is processed.

Repeat orders - for businesses offering subscription based models

Single-click payments - as the payment processor already stores the customer's details securely, the merchant just needs the customer to enter their card security code (also known as CV2 or CVV) to validate the payment. This keeps payments more secure whilst improving the customer's overall experience.

And finally…
Don't forget your security policy

If you're doing all this work to keep your website and your customers safe, you should be shouting about it.

If you don't already have a security policy on your website, you should think about creating one. It should set out details of how you manage payments and card security on your website, as well as your policies for data security; for example, user registration and password retrieval; data capture, storage and back-up; SSL browser encryption and any other forms of sensitive data transmissions. Make it as easy as you can for potential customers to access the policy by including links to it throughout your website.

You should also allocate a stakeholder within your organisation who will be responsible for monitoring that the policy is enforced and ensuring that it is updated as your business evolves.

For more information on fraud or other Sage Pay services, please visit our website www.sagepay.com