The Fraud Landscape

Contents

Intro

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 landscape, payment card regulations to help you maintain secure systems and tips on how to mitigate fraudulent transactions.

The Fraud Landscape

The battle against fraud continues. In our Payments Landscape 2014 report, we found that this year over 40% of businesses lost money as a result of fraud and with the average loss to a mid-sized business at over £11,000, it's no laughing matter.

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 offer you basic fraud tools. These are:

- **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.

Despite the worrying numbers of businesses hit by fraud, our Payments Landscape report found that 39% of businesses don't spend anything on fraud prevention and instead rely on the free tools provided by their payment gateway. While these tools should be sufficient for smaller businesses, if you need a bespoke fraud prevention solution, these are available through third party suppliers.

ReD Shield®

Sage Pay partners with ReD, a specialist provider of fraud prevention solutions for all payment transaction types, that has solutions to fit every type of business.

Red Shield detects and manages payment fraud, ensuring that valuable transactions are processed while potentially fraudulent ones are identified and isolated.

The benefit of ReD Shield is that it can work in conjunction with your existing in-house fraud screening tools, reducing the time and costs associated with manual reviews, whilst protecting your businesses from losses to fraud.

For more information on ReD, please visit www.redworldwide.com.

High Risk countries

The top 12 international sources for online fraud are: Ukraine, Indonesia, Yugoslavia, Lithuania, Egypt, Romania, Bulgaria, Turkey, Russia, Pakistan, Malaysia, and Israel.

Getting the Fraud balance right

When it comes to fraud, businesses need to get the balance right. Immediately rejecting a transaction that looks suspicious isn't always the right course of action.

It's worth keeping in mind that for every extra action a consumer is asked to make - you risk losing a sale. So before tightening your security controls, consider the following the below 5 steps in order to protect your genuine customers…

5 ways to reduce fraud

1. 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.

2. Be extra cautious of 'high-risk' countries. This is especially relevant as more e-businesses than ever are expanding their reach. With Sage Pay's fraud screening tools, you can block all or some of these high risk countries

3. Address verification (AVS) and card security code (CV2) checks should be implemented as a matter of course. Set fraud screening rulebases to ensure no suspicious transactions slip through. As a mid-sized business, you may or may not have the resource available to check individual orders coming through the system. If you don't, your payment provider should provide the functionality to allow you to set rules based on the value or volume or orders.

4. 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.

5. Think about investing in a bespoke service from a fraud screening specialist.

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 emphasise the need for encryption, access controls and firewalls. How stringent these are depends on which level you will be required to reach.

PCI requirements

Build and Mantain a Secure Network

- **Requirement 1:** Install and mantain 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 Payments Landscape 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.

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 our Payments Landscape report, 35% of mid-sized businesses reported that they had saved between £1,000-£20,000 off their PCI costs by using tokenised payments, with a further 11% saving upwards of £20,000.

And these savings aren't the only benefit of tokenised payments. This technology can also facilitate a single click checkout. As the payment processor already stores the customer's details securely, the merchant just needs the customer to enter their card security code (CV2) to validate the payment. This keeps payments more secure whilst improving the customer's overall experience.

For more information on fraud or other Sage Pay services, drop us an email http://www.sagepay.co.uk/email-us or give us a call on 08455916390.