Why your PSP should be your best defence against fraud

July 2017

processing.paysafe.com

Paysafe

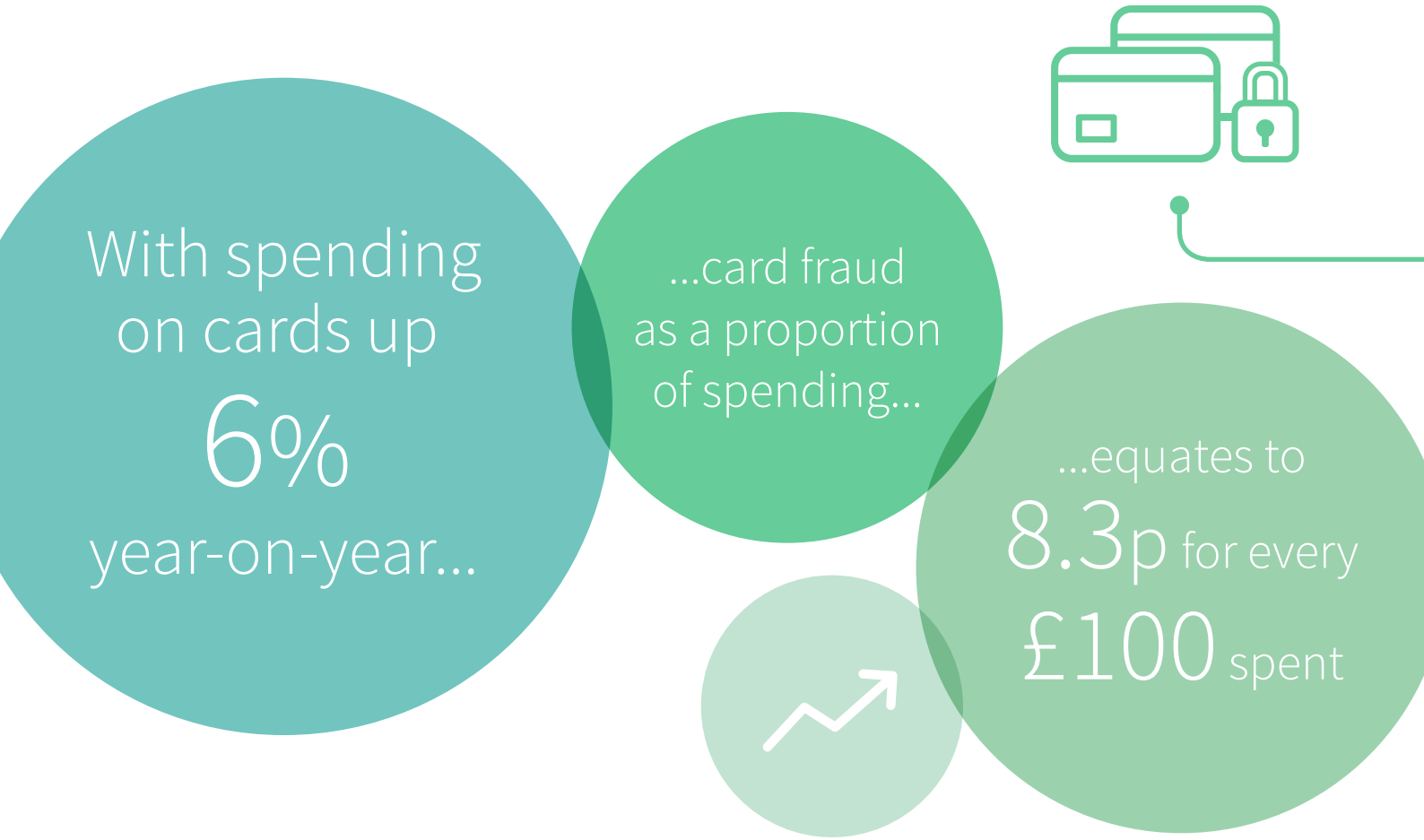
Why your PSP should be your best defence against fraud

If recent crime statistics have taught us anything, it's that fraud has reached epidemic proportions. According to latest Office for National Statistics (ONS) data[i], fraud offences are up four percent year-on-year in England and Wales, totalling 3.5 million incidents in total over one 12 month period.

Further data[ii] released by Financial Fraud Action UK (FFA UK) showed that payment card fraud accounted for losses of £618 million in 2016, an increase of nine percent over the previous year. With spending on cards up six percent year-on-year, this means card fraud as a proportion of spending equates to 8.3p for every £100 spent.

Payment card fraud accounted for losses of £618 million in 2016.

These numbers considered, it's never been more critical for merchants to tackle fraud head-on, and work with their PSP to ensure a robust fraud defence strategy not only exists, but is also reviewed regularly to optimise legitimate transactions. This report examines the challenges facing merchants when it comes to fraud prevention, and explores the methods they can utilise in order to implement a successful fraud strategy.



So you think you know fraud?

With so many different types of fraud prevalent in online transactions, the odds are often stacked against merchants. Understanding the ways in which fraud can be committed is the first step in combatting it.

Combatting true fraud

The term 'true fraud' refers to fraud that is committed with malicious intent, and comes in many different guises:

- **Clean fraud:** A method whereby a fraudster has been able to carry out a purchase by using a complete profile of stolen data that makes the transaction appear legitimate, rendering the merchant unable to identify that fraud has been committed.

  Often, a fraudster will perform tests by making low-value purchases to determine whether the stolen data is able to dupe fraud prevention systems. By possessing a great deal of information about the rightful owner, and then applying methods that manipulate the transaction, this type of fraud can be incredibly difficult to prevent.

- **Identity theft:** The use of sensitive personal information fraudulently in order to conduct payment fraud.

  Appropriating the data required to commit identity fraud is achieved in a number of ways; by using data from sources that have been compromised; by hacking sites to steal sensitive information; phishing scams; pharming, which works by redirecting unsuspecting customers to fraudulent websites that appear to be legitimate; and opportunistic fraudsters who intercept credit cards sent in the mail, or when left unattended by the rightful owner.

  Credit cards are often the most popular target for identity fraud, and are commonly used in Card Not Present (CNP) transactions.

- **Account takeover fraud** is similar to identity theft; however, the fraudster may only have access to limited information such as a name and credit card number. In this scenario, a fraudster poses as a genuine customer, and gains control of an account, changing a few details such as email or address, allowing them to make transactions.

  While these types of fraud can be difficult to detect, they account for approximately 30%[iii] of all fraudulent transactions.

Often, a fraudster will perform tests by making low-value purchases to determine whether the stolen data is able to dupe fraud prevention systems.

Combatting chargeback fraud

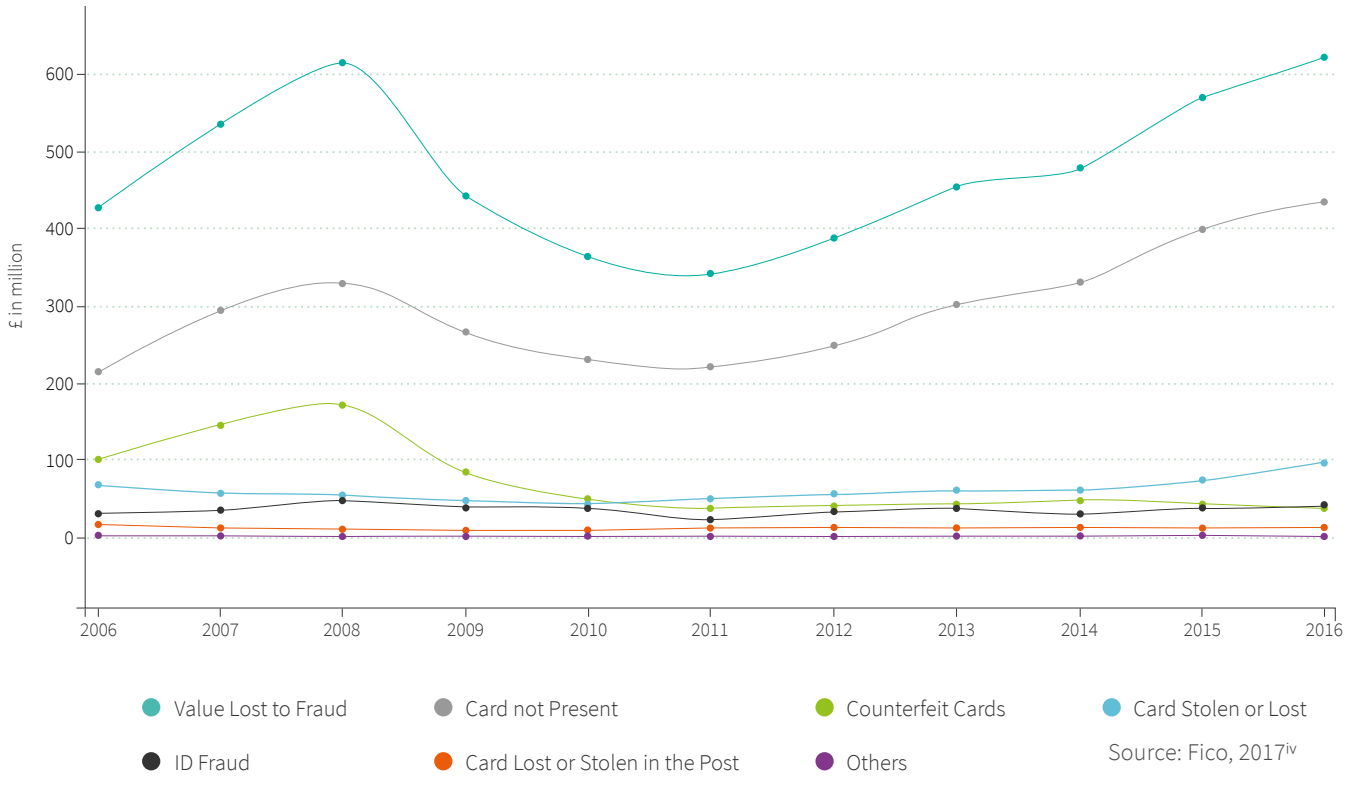
A much bigger challenge for merchants is chargeback fraud - which comes in two forms:

- **Friendly fraud:** As the name suggests, friendly fraud is unintentional, as it involves no malicious intent. Reasons cited as the most common causes of friendly fraud include family members making purchases without the cardholder's permission, confusion surrounding merchant return policies, and consumers forgetting when they have made a purchase, or not recognising activity in their account, resulting in them cancelling the payment without first contacting the merchant to resolve the issue.
- **Chargeback fraud:** In contrast to friendly fraud, chargeback fraud is intentional and relates to a fraudulent request for a return or refund in the form of a chargeback. The transaction passes fraud prevention, but is then disputed by the cardholder in an attempt to recover the cost of the product or service. This may be denial that products or services were delivered or were damaged in transit, when in fact they were delivered to the recipient in perfect condition.

Friendly fraud and chargeback fraud can be incredibly hard to prevent, and disputes can be a time-consuming process for merchants to manage.

This is where working with an acquirer that is proactive in identifying and mitigating chargebacks can be extremely beneficial for merchants, as it allows them to identify potential issues before they arise, which saves a lot of time, money, and stress.

Increase in fraud YoY in the United Kingdom



Source: Fico, 2017[iv]

Leveraging your PSP to stop fraud in its tracks

Fraud rules, which are also referred to as threshold rules or velocity checks, exist to detect and prevent fraudulent transactions before they occur.

These rules are triggered when a user performs an action that possesses fraudulent traits; making an abnormally large number of transactions in a short period of time, or a transaction where the billing country and the IP country do not match, being just two examples.

False positives lead to legitimate transactions being declined, resulting in lost revenue for the merchant.

In most cases merchants have full control over these rules - when they trigger and what the trigger thresholds are - and they can be adapted to meet specific business requirements.

However, without the support of an experienced acquirer, making changes is risky; by not having adequate fraud rules in place the likelihood of fraud increases, whilst too many fraud rules can result in false positives.

It is therefore important for merchants to work closely with their acquirer to determine the right balance of rules for their business specifically, based on business model, transaction types, and low/medium/high risk products. A dedicated fraud and chargeback team can also give merchants comprehensive advice to develop a strategy that uses a fine balance of rules to stop fraud, whilst allowing the 'good transactions' to filter through.

One size does not fit all

Different businesses need different fraud rules in place, based on industry, the products or services being sold, and average transaction size. For example, a high-value, low-volume business such as an online travel agent, will require a different set of fraud rules to a low-value, high-volume business, such as an online coffee shop.

The Global Fraud Index report released by PYMNTS[v] in May 2017 revealed that high-value orders have the highest fraud rates, with orders of $500 (approx £385 at time of writing) or more are almost 20 times more susceptible to fraud than lower-value transactions.

With this in mind, fraud rules simply cannot be effective when implemented with a 'one size fits all' approach. Determining which fraud rules are applicable to a specific merchant requires the knowledge of a merchant acquirer who is able to offer a significant number of rules to assist in fraud and chargeback prevention.

Fraud rules simply cannot be effective when implemented with a 'one size fits all' approach.

As part of the way in which fraud rules are managed, an acquirer will look at chargeback and fraud trends to determine if any settings need tightening up. They will identify the trends and determine what (if anything) needs amending to resolve either a short/medium/longer term problem. Sometimes quick fixes can resolve issues promptly; however sometimes risk rules need to be in place for longer to alleviate any longer-term issues.

Finally, established merchant acquirers will have access to a database that has been in production for many years, allowing the system to evolve over time while building significant lists of negative fraud data to allow merchants to trade, safe in the knowledge that the database is working in the background. This allows the merchant to concentrate more on the good transactions whilst the acquirer operates in the background protecting merchants from the bad transactions.

Orders of

$500

or more...

...are almost

20x

more susceptible to fraud than lower-value transactions.

Having the right tools is critical

Merchants may find choosing an acquirer to be a daunting task, particularly when there is such an abundance of fraud and chargeback prevention tools on the market.

Many acquirers are new to the industry, or have limited experience and interaction with the e-commerce space. Therefore, merchants should only partner with an established acquirer that is able to provide the experience, development, and system learning of tools that have been in production for almost as long as e-commerce itself.

An established acquirer should provide the following state-of-the-art services and tools to safeguard merchants against fraud:

- Customizable Risk Rules Engines
- Address Verification Systems (AVS)
- CVV and CVV2 matching
- Positive and negative database checks
- Geo-IP address verification
- 3DS
- BIN number validation
- Transaction velocity monitoring
- Global device intelligence
- Identity Verification

Acquirers should also provide insight into fraud prevention methods, determine trends in fraud, identify issues in a proactive manner, and provide the guidance, tools and expertise to counteract the issue as well as provide long term fixes.

As fraud continues to grow, and as fraudsters become increasingly sophisticated in their methods, merchants face increasing pressures to mitigate the risks. Having a robust fraud prevention strategy in place is no longer optional, but critical for businesses that intend on succeeding in a world fraught with challenges.

Trade in confidence with Paysafe

Paysafe has over twenty years of experience managing e-commerce payments, with a highly experienced global Fraud and Risk Management division. We also service businesses of all sizes with a comprehensive portfolio of fraud, risk and chargeback management solutions to review transactions in real-time, dispute chargebacks on the merchant's behalf and provide strategies to limit future vulnerability. We also partner with industry-certified fraud management partners to give merchants total confidence that transactions can be carried out securely.

To find out more please visit our website

References

i https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingdec2016#whats-happening-to-trends-in-fraud

ii https://www.financialfraudaction.org.uk/news/2017/03/30/financial-fraud-data-for-2016-published/

iii https://chargeback.com/true-fraud-vs-chargeback-fraud/

iv http://www.fico.com/europeanfraud/united-kingdom

v http://www.pymnts.com/global-fraud-index/

Paysafe