> Within CNP fraud, ecommerce fraud took up roughly £140.2 million of the total figure in 2012, accounting for around 57% of total CNP fraud.

Fraud

Payment industry fraud and the measures taken to combat it are key topics of interest and concern in the current UK trading climate. For an aspiring online retailer looking to trade in the UK, understanding the forms this fraud can take, its prevalence and recommended preventative measures are all vital steps in ensuring a safe and successful business for both you and your customers.

OVERVIEW

Between 2011 and 2012, total fraud losses on UK cards increased by 14%, in 2012 accounting for £338 million. This should, however, be viewed in context, as at its peak in 2008 total fraud losses on UK cards accounted for £610 million, which overall shows a decrease of 36%. In 2012, card fraud losses against total turnover came in at 0.07%.

According to Financial Fraud Action UK, in 2012 Card Not Present (CNP) fraud accounted for around 63% of card fraud losses in the UK, costing £245.8 million. Alongside this:

- Card ID theft accounted for 8%
- A lost or stolen card accounted for 14%
- Counterfeit cards accounted for 11%
- Mail non-receipt accounted for 3%

Within CNP fraud, ecommerce fraud took up roughly £140.2 million of the total figure in 2012, accounting for around 57% of total CNP fraud.

Above average fraud rates have been recorded to occur in mobile transactions, so merchants need to ensure that they are well prepared for the growth of this sales channel. Fraud rules need to be tailored to meet the specific challenges of mobile fraud detection.

INDUSTRY MEASURES FOR PLASTIC CARD FRAUD

Plastic card fraud levels in the UK have vastly decreased since the introduction of more advanced security measures, such as chip and PIN technology in 2008 which resulted in counterfeit fraud accounting for just £42.1 million

The UK has recently seen the introduction of online fraud prevention initiatives like American Express SafeKey, MasterCard SecureCode and Verified by Visa, which require cardholders to register their cards and create passwords for provision when shopping online with participating retailers, adding an extra layer of protection through two-factor identification.

in 2012, a quarter of what it was before the chip and PIN system was implemented. Levels of fraud on the high street have also fallen by 75% since 2004 as a result. The fraud attempt rate for cards issued in the UK is broadly similar to that of most other major European countries.

Although card payments are heralded as a very safe way to pay for goods and services in the UK and overseas, it is still very important to make every effort to protect against fraud. In order to reduce losses associated with plastic card payments fraud, a UK merchant can subscribe to the Industry Hot Card File, which contains information on over 7.2 million payments cards that have been lost, stolen, or comprised. A participating retailer can check a customer's payment card against the database as part of a normal transaction and will be altered if the card details match any of those on the database.

INDUSTRY MEASURES FOR CARD NOT PRESENT FRAUD

Internet shopping has been made considerably safer through the introduction of 3D secure - the online equivalent of the chip and PIN system. The UK has recently seen the introduction of online fraud prevention initiatives like American Express SafeKey, MasterCard SecureCode and Verified by Visa, which require cardholders to register their cards and create passwords for provision when shopping online with participating retailers, adding an extra layer of protection through two-factor identification.

Recent years have also seen the introduction of the automated address verification service (AVS) and the card security code (CSC). These checking systems provide extra protection against fraud by endowing participating businesses with additional information to help identify fraud risks. Respectively, these initiatives allow retailers to verify the billing addresses of cardholders and cross-check the security code that is contained on the signature strip at the back of a payment card.

Banks and card companies are also implementing increasingly sophisticated fraud detection systems, for example using consumer profiling to identify unusual spending patterns or atypical behaviour in a consumer, helping to identify potentially fraudulent transactions. The card company will contact the cardholder to enquire about the transaction in question, and can instate an immediate card block if necessary.

Adding to the above, there are a variety of additional initiatives in place to reduce fraud both in the CNP and the wider payment industry context, including ID verification techniques, more advanced fraud screening tools, free security software for consumers and partnerships between banks, interested companies and governmental bodies which aim to monitor, advise and inform and implement new fraud-fighting strategies.