

Online payments

E-commerce struggles to secure the checkout

As more and more purchases migrate online, the problem of online payment fraud grows more acute. Banks and card issuers face a major challenge to secure the e-checkout and sustain the development of the internet economy.

The rise and rise of online commerce

In a desperately gloomy environment for retailers, online sales are the one area providing some degree of comfort. For example, in the 22 weeks to December 27 2008, bellweather UK retailer John Lewis reported an overall decline in sales of 4.5%. However, while many of its large department stores reported double-digit falls in sales, sales at johnlewis.com showed an increase of 15.0%.

Retailing is of course only one of the sectors where consumer transactions are migrating online. From reserving hotel rooms to booking airline tickets and placing bets, all have become to some degree internet-based activities.

For some businesses, such as the budget airlines, almost everything other than the flight now takes place online. Ryanair, which recently announced the closure of all its airport check-in desks by the end of 2009 in favour of online check-in, reported that 97% of passengers already book online and 75% use the internet to check in.

The rise and rise of online fraud

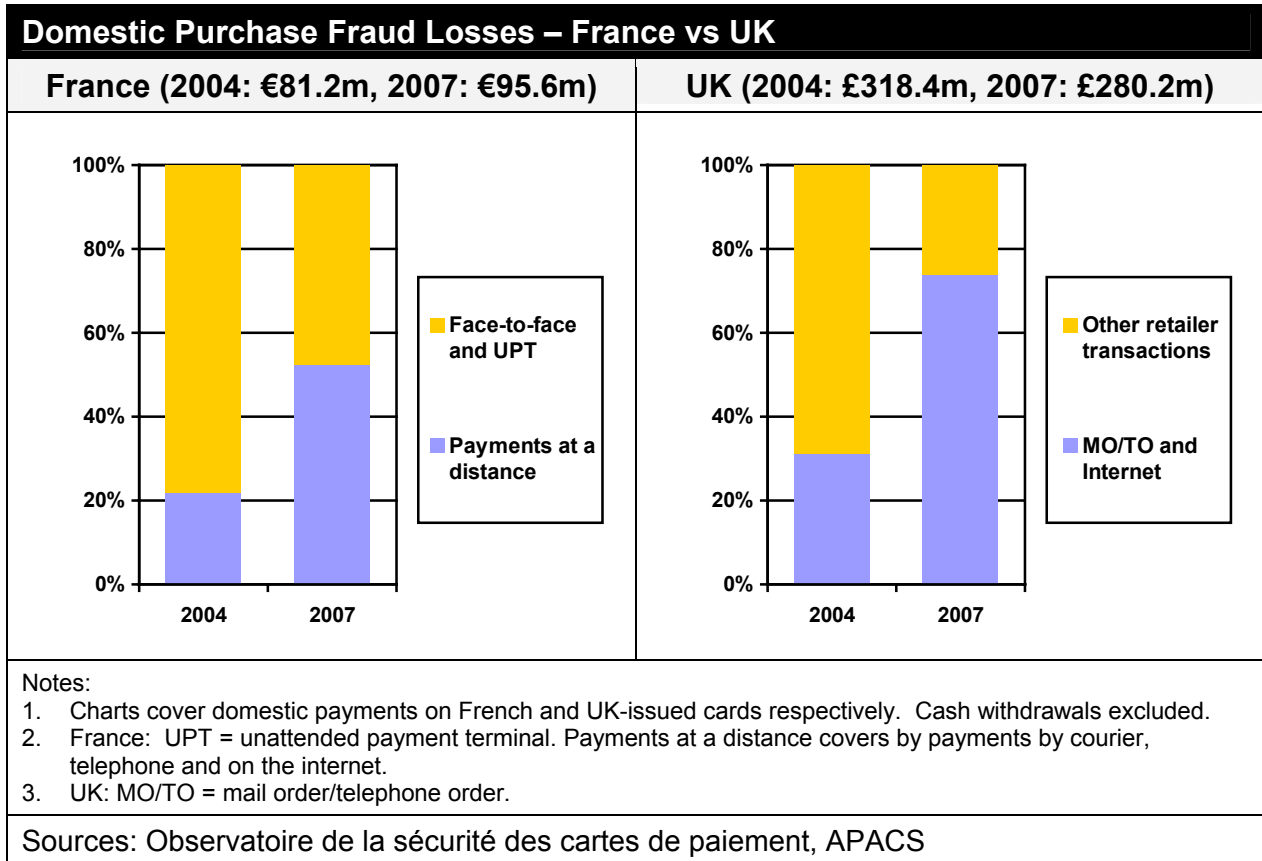
However, despite its relentless expansion, e-commerce is struggling with a major problem – namely the vulnerabilities surrounding online payments.

In many countries, credit and debit cards are the default means of making internet payments. Indeed, with some online merchants, payment by card is effectively the only option. But a recent comparison of payment card fraud across three of the largest European countries underlines just how vulnerable online commerce has become to the fraudulent use of cards.

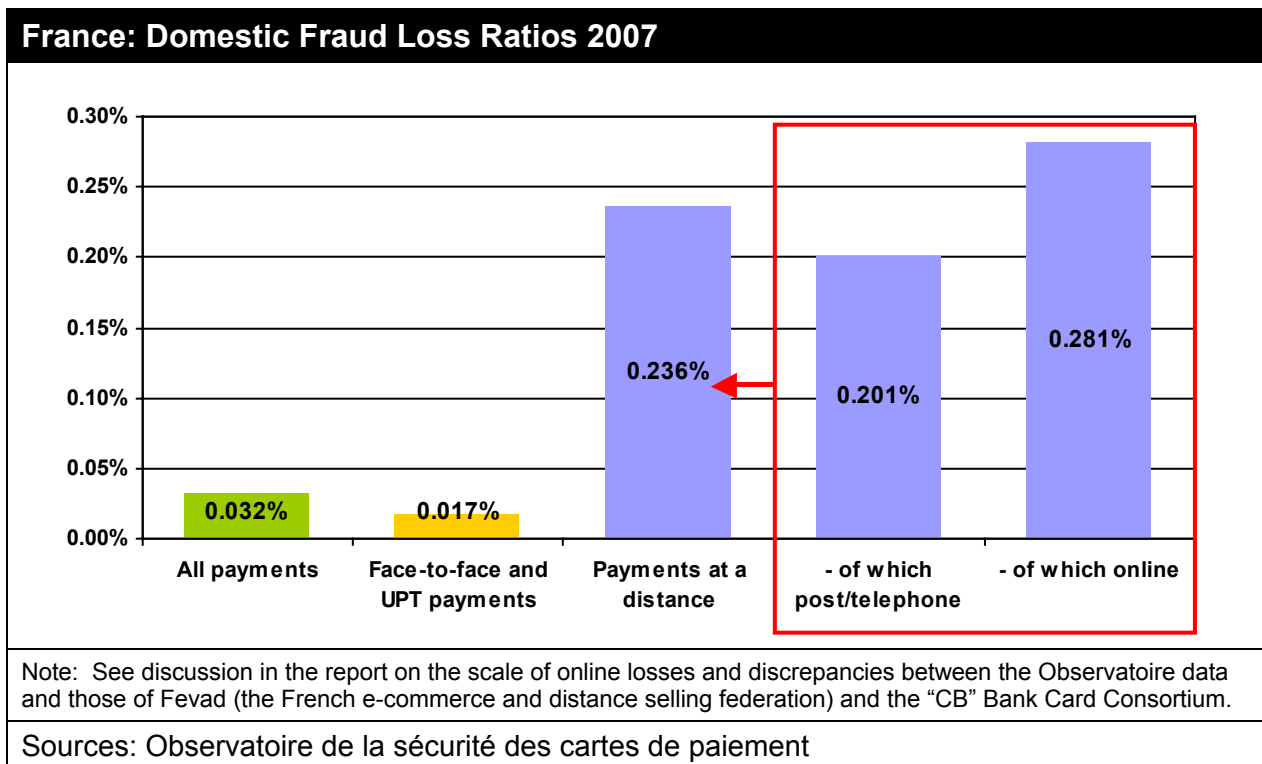
The scale of the problem is most evident from the data available for France and the UK. The adoption of Chip and PIN in the UK has significantly curtailed losses from face-to-face card payments in shops and other outlets. Losses of £73 million in 2007 compared with peak losses of almost £220 million in 2004. France, as the earliest adopter of chip on cards, had already secured a significant reduction in losses from face-to-face transactions. It has now followed the UK in upgrading its cards and acceptance infrastructure to the international EMV standard.

But Chip and PIN offers little protection online, where only the card details rather than the physical card are needed to undertake a transaction. As a result, card details alone have become much more valuable, with their theft now the most significant method of card compromise. And in those countries where EMV has been implemented, so raising the barriers to use of a physical card, it pushes card fraud online.

The numbers for both France and the UK underline the scale of the switch from face-to-face to online losses. As recently as 2004, payments at a distance (mail order, telephone order, and internet) accounted for only 21.8% of total domestic losses on card purchases by value in France and only 31.3% in the UK. By 2007, losses from payments at a distance accounted for just over half of domestic losses in France in 2007 and almost 75% of domestic losses in the UK.



In fact, striking as these numbers are, they understate the scale of the problem of online fraud. The French data includes loss rates – ie fraud losses as a proportion of the value of card payments – broken down by different types of card payment. While there is some dispute over just how high French loss rates on online payments were in 2007, even the lowest estimates suggest they were seven to eight times higher than those of face-to-face payments.



Measures to combat online fraud

Looking at measures to combat online fraud, lists of lost and stolen cards are of little help if, unknown to the cardholder, only the card number has been compromised. The three-digit CVV number on the card's signature strip has provided some measure of protection against fraudsters in possession of the card number and expiry date, but not the physical card. And banks use address verification and transaction monitoring systems to identify and decline potentially fraudulent transactions, though the latter risk irritating genuine customers if what prove to be non-fraudulent transactions are declined.

However, the scale of online losses underlines the need for building additional security into the online purchase process. Banks and the card networks are strongly promoting the adoption of MasterCard SecureCode and Verified by Visa (VbyV). Once the customer has entered his or her card details, he or she is transferred to a secure window provided by the card issuer requesting the SecureCode or VbyV password.

The industry claims their adoption is now growing strongly. In September 2008, UK payments association APACS reported that more than 25 million credit and debit cards are now signed up to the two schemes, compared with 10 million registered cards in August 2007 and 3.6 million cards in August 2006. And in November 2008, Visa Europe reported a 104% growth in European usage of Verified by Visa in the past two years. In the last 12 months alone, it said VbyV handled over 100 million European transactions and U.S.\$21 billion in payments.

Future measures

However, despite the chargeback incentives, some major online merchants still have to adopt the schemes while some cardholders complain that their effect is to unfairly transfer liability to them for fraudulent transactions. And even assuming widespread adoption of SecureCode and VbyV, they retain the vulnerabilities of password-based systems. It is clear that further security measures will be needed – and needed quickly.

Visa for example is already exploring enhancements that generate a unique code for each transaction. Several banks in Europe are piloting Visa cards which incorporate an alpha-numeric display and a 12-button keypad. When used with VbyV, rather than entering a password the consumer enters their PIN into the card which creates a unique code for each transaction. Several banks in Asia are piloting a similar mobile phone-based system for the use of Visa cards online. The enhanced VbyV service generates a one-time password sent to a cardholder's designated mobile number via a text message.

Use of phone-based measures are already starting to be implemented, including so-called Out-of-Band Authentication (OOBA) solutions that require user or transaction-specific details to be entered via phone separately from the online side of the process. HSBC, for example, recently announced its adoption of Authentify's OOBA services to automatically authenticate online users attempting certain transaction against HSBC accounts.

However, there is no magic bullet. Additional security measures entail additional costs and risk overcomplicating the online purchase process for both cardholders and merchants. Cardholders want both security and convenience, when the two often pull in different directions. And convenience is vital to e-commerce merchants who fear losing business if too many layers are added to the payment process. All of which underlines the challenge of containing online fraud without losing the ease and efficiency of online shopping.

Notes

An earlier version of this bulletin first appeared as a Capco Institute Bulletin.

The bulletin draws on a recent report, *Online and Overseas*, comparing payment card fraud in France, Spain, and the UK. For a complimentary copy of the report, email pwelch@bankecon.com

Copyright

Copyright © Peter Welch 2009.

The briefing has been produced by Peter Welch, a self-employed consultant resident in Italy. Partita IVA (VAT number): 05613230480. Peter Welch produces banking research and analysis under the BankEcon name. Reproduction of the briefing is permitted so long as the source is acknowledged.

Disclaimers

While every effort has been made to ensure the accuracy of all data and information in this report, the author cannot accept responsibility for any errors or omissions, no matter how caused.

This briefing is not investment advice. It should not be relied on for such advice or as a substitute for professional accounting, tax, legal, financial or other advice as appropriate. It is not an offer to buy or sell securities or a solicitation of an offer to buy or sell securities.