Keeping the evolving omni-commerce world secure

Consumers don't care how they access an online shop, but they do expect the same product offering, level of service, security and ease of use that they get from a standard website experience, no matter whether they are accessing the shop via a mobile tablet or web store. Retailers are expanding into an increasingly omni-channel world, selling across multiple channels and geographic markets, and via multiple touch points, including mobile apps, social media, interactive TV and, of course, the web. Secure and seamless payments across all these channels can result in more efficient operations and the most appealing customer experience, but the increasing complexity around taking payments via 'card not present' methods across multiple channels makes it difficult for retailers to assess the validity of each purchase and in turn to authenticate customers' identities.

CyberSource's 2013 UK eCommerce Fraud Report found that 44% of online merchants operate a mobile site, but 71% of these only use their standard fraud screening used on their web commerce channel, even though it’s entirely separate to their mobile channel. This is a major problem, as some fraud checks that work for e-commerce channels may be counterproductive, irrelevant and potentially misleading when applied to other channels, such as mobile. For example, use of IP address geolocation by merchants when looking at web orders is standard practice, but if applied to the mobile world can lead to misleading results.

As retailers offer more channels the complexity and risk associated with the management of payments exponentially increases. To effectively tackle increasing cybercrime across multiple channels retailers must start joining up their back-end processes. This can provide a single view of the customer, giving retailers the ability to spot abnormal behaviour and prevent fraudulent activity across multiple platforms without affecting the customer experience.

Surprisingly, CyberSource's aforementioned recent report revealed that as many as 48% of merchants do not track fraud by channel at all. An increasing number of channels mean that retailers have to process a larger amount of data. In effect, there’s a pipeline of payment activity that intersects multiple business processes throughout the order management lifecycle — and so there are more opportunities for fraudulent payment data to enter the process. Fraudsters understand that there are such gaps to exploit between payment channels, and until retailers take steps to tighten those gaps they will be putting their business and their customers at risk. Retailers' back-end systems must be tightened up to begin to tackle fraud rates, and the first step is tracking payment activity across their different channels so that anti-fraud measures can be surgically targeted to the channel being attacked by fraudsters rather than bluntly across all channels.

Future-proofing for the omni-commerce world can be a demanding task for a rapidly growing retailer. However, working with a service provider that processes payments on the retailer’s behalf helps make the task easier, as customer data is taken out of the retailer’s hands and stored remotely and securely. Hosted payment acceptance — when combined with tokenisation — removes sensitive payment data from the merchant’s environment, cutting the risk of a data leak and preventing fraud.
Ieak-A token is provided to the retailer for storage in their planning system for future transaction processing and customer service activities, but the retailer never has anything more than the last four numbers of anyone’s card details. Sensitive payment data is not stored anywhere on the retailer’s system meaning retailers can deliver a better customer experience without ever touching, storing or handling payment data.

Increasingly retailers are choosing such systems, rather than processing payments in-house, for three key reasons:

1. It’s safer – Retailers who centralise their payments don’t have to rely on tracking down all the payment data, locking it down, or monitoring human behaviour with policies and procedures. The data isn’t there. There’s nothing to steal.
2. It’s less complex – A single platform from which to manage payments enables retailers to significantly reduce key management and payment security policy enforcement. As there’s no payment data interaction, and no need to procure or manage the layers of software and hardware, the entire process is much simpler to manage.
3. It’s easier and less costly to certify – Though PCI compliance shouldn’t be the sole focus of any retailer’s effort when it comes to efficient payment systems, it remains extremely important.

To effectively, efficiently and securely future-proof their businesses for the omni-commerce world retailers must take a holistic view to managing the payments process and provide customers with a seamless, secure and consistent checkout experience, whatever the channel. The eCommerce landscape used to be straightforward, but now with so many channels to cater for and manage, retailers need to make sure they put forward-thinking measures in place so that they don’t fall short.