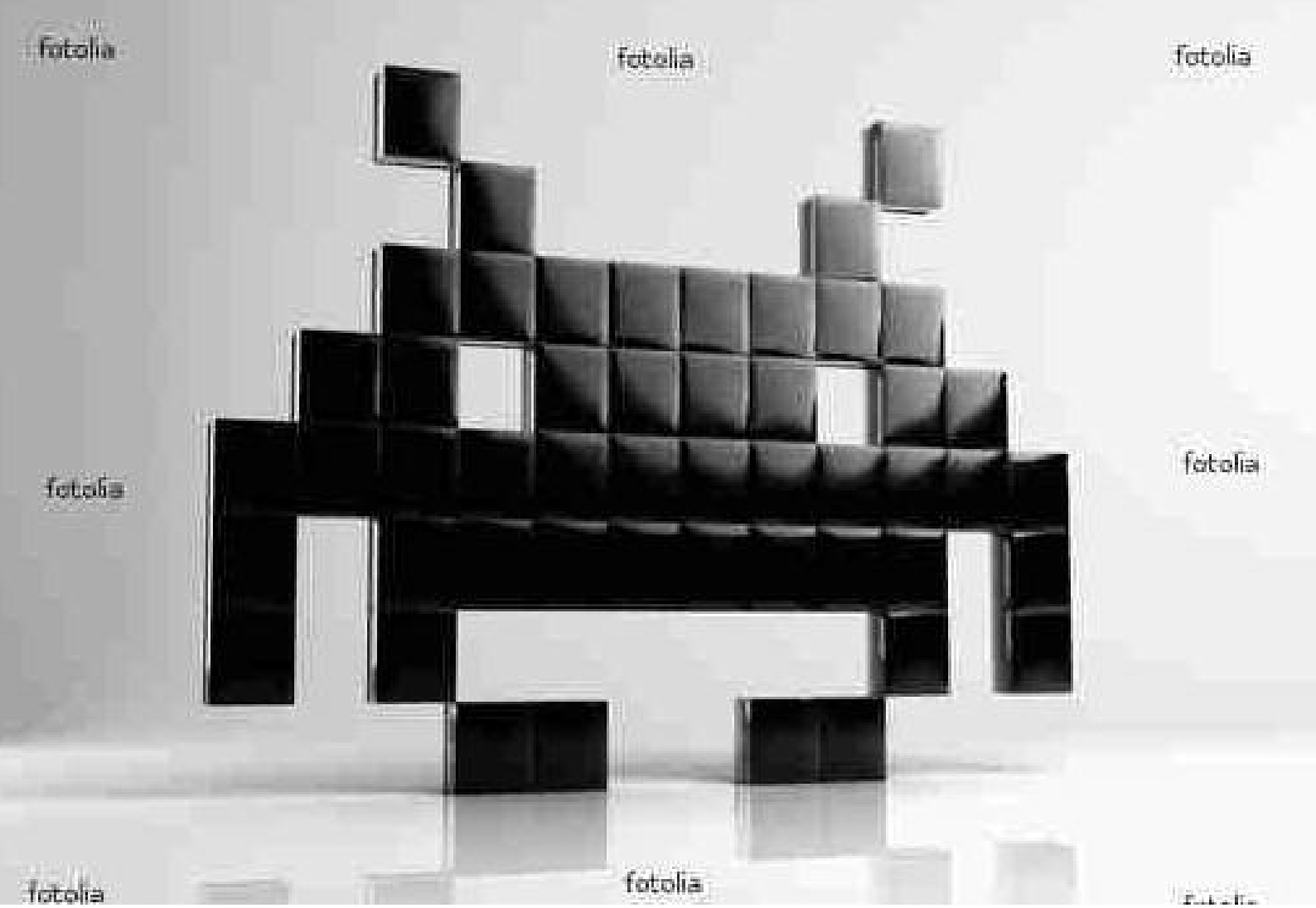

War games

Payment processing and fraud systems are 'invisible' to all but a very few within many businesses. However, they're fundamental to effective ecommerce, as Arif Mohamed discovers.

EVER BUILT and fortified your own castle? If so, you will know that you can choose from a range of materials to build the walls and weapons to line the tops. You can even choose to have fighter orcs and dragons hidden behind the walls, just in case.

Building an e-commerce site is very much like that, obviously without the orcs and the dragons. As you prepare your castle – your online estate – to do business with the outside world, there are fortunes to be made, but you can be sure the cyber criminals will try their best to breach the walls.

As a result, online retail has become both lucrative and hazardous for businesses.

Lucrative because consumers are choosing to spend more of their cash online. This Christmas, gift buyers were expected to spend £4,000 every second, with one-day sales expected to top £350m, trampling the £320m spent on the busiest day last year.

Hazardous because fraudulent transactions and card theft remain high, causing migraines for online vendors, customers and banks. According to banking industry figures released in October, UK online banking fraud losses rose 55 per cent to hit £39m for the first half of 2009.

Consequently, businesses have found themselves shouldering the burden of fraud, along with other financial partners, whilst educating their customers to be more careful in the way they use their cards on the web.

Back to the wargaming illustration. Good payment processing and fraud systems are the orcs and dragons hiding behind the walls of your castle. But rather than being a nice add-on, they have become fundamental to the fabric of our e-commerce systems.

These processing services appear 'invisible' to all but very few within the business, but they are growing more powerful and savvy, as they battle to root out fraud.

Many companies shy away from doing business online, partly because of the fraud factor.

Eclipse Internet, a business ISP, says that few businesses are maximising the web's potential as a sales channel, due to concerns over technical complexity and the risk of online fraud.

"It staggers me that there are still thousands of SMEs that don't have the facilities for online shoppers to buy products or services on their websites," says Clodagh Murphy, director of Eclipse Internet. "Far too many SMEs see the web as just a marketing channel rather than a sales opportunity."

He adds that the benefits of e-commerce vastly outweigh any potential pitfalls, and to miss out is to sacrifice a huge opportunity to succeed in a rapidly-changing marketplace.

It is a valid concern about web-based transaction systems getting more complex, and the fraud risk rising.

But the big difference between the way we do things now, as opposed to in the early Nineties, is that the orcs and dragons – the card processing and anti-fraud systems - are outsourced services, and they are helping us to win the battle.

Businesses no longer have to develop and host their own big and costly online retailing platforms, as before, although there are a few larger online retailers that still have their own.

Instead, retailers just need to link up with a PayPal or a Sage Pay, and get them to deal with the customers and the banks for them. That way, they don't need to invest in payment processing technology, or even hold any customer data, making data compliance somebody else's problem.

BEHIND THE SCENES

So, what exactly is going on behind the scenes whenever a customer makes a transaction on your website? Every online payment, or attempted transaction, triggers a sequence of events that spans huge distances.

The payment flow goes like this. The customer uses their card to buy something from your website's shopping basket. This sends a message on a long, but lightning-fast journey, across at a number of parties. The message will hold some details about the customer, such as their name and a bit of their address, and the value of the transaction.

First this packet of information will go to the e-tailors bank, the 'merchant acquiring bank'. This organisation will approach the bank responsible for the customer's card, the 'issuing bank'.

The issuing bank will do its checks and send the message back to the acquiring bank, which will accept or decline the purchase and tell the customer the verdict.

There's just one more thing to add to the picture. The organisation that transports the message between the customer and the banks is the payment processing service provider.

Among the leading bank-independent ones are Sage Pay, PayPal, Optimal Payments, PacNet Services and E-Clear, which was recently in the news as the processer of online payments for Flyglobespan, Scotland's biggest airline.

The banks also have their preferred processing service arms. Lloyds has Cardnet Merchant Services, The Royal Bank of Scotland has RBS WorldPay, and Bank of Scotland favours its Streamline.

There are advantages of choosing a bank-agnostic payment processer, argues Sage Pay's head of business development, Joe Robey, as you would expect him to. He explains that Sage Pay, which was formerly Protx, has forged links with almost a dozen banks. But to do this, it has invested big money on the networking and server technologies that allow it to link with them, on behalf of its customers.

The physical connection may differ for each issuing bank, with some allowing the transaction details to travel over IP, but others restricting traffic to hard-wired X.25 lines. This is an underground network of cables used extensively by the banks and ATMs in the Eighties.

Robey says that Sage Pay and other independent service providers like it can offer affordable payment processing capabilities to smaller businesses. This means customers can concentrate on their core business, rather than on the complexities of payment processing.

The main reason why payment processing is a complicated affair is because the processors have to be accredited separately with each different acquiring bank.

They also need to keep up with regular audits, strict tests, and changes to the bank's payment mechanisms, as well as data protection and banking requirements.

FRAUD BUSTING

As well as staying on top of banking and government compliance issues, payment processing intermediaries and banks are introducing more and more anti-fraud measures

Soul trader

Ever thought anyone could make serious money selling shoes over the web? Well, Fitness Footwear [www.fitnessfootwear.com] has kicked its competition to touch.

The firm's slick website, free delivery, easy returns, and great service have helped it grow from a one-page site into the largest independent sports footwear retailer in the UK. Underpinning Fitness Footwear's site is Sage Pay's processing transaction service.

Fitness Footwear co-founder, IT worker Luke Barlow, explains that in 2005 he built a one-page website for his brother Glyn to sell shoes online. The brothers were approached by a national supplier and Fitness Footwear rapidly grew into a successful business.

In four years Fitness Footwear has become the leading supplier of brands such as Fit Flops, and was a recent finalist for the country's prestigious Drapers award for footwear e-tailer of the year.

The firm started off using one payment service provider, but soon switched to Sage Pay, looking for a more reliable alternative which offered good security and anti-fraud features, says Luke. He adds that it was attracted by Sage Pay's low and predictable monthly fees, easy-to-use administration tools, and good customer service reputation.

Integrating the payment service into the site's shopping cart was straightforward, says Luke, with the majority of the setup being done online. Sage Pay supplied 24/7 support and an integration kit to help with the process.

Prior to using Sage Pay, fraudulent transactions were a big problem. "We were haemorrhaging substantial quantities of cash to fraudsters, which could be better spent on developing our range of products and enhancing the online shopping experience of our customers", says Luke.

However, Sage Pay's high levels of fraud screening have helped to boost customer confidence whilst driving down fraud. As a result of the switch, the business saved £1,200 overnight, claims Luke.

"When you consider how much we were losing to fraudulent transactions, the processing fees paid to Sage Pay have been worth every penny in helping us to save money for expansion in other areas," says Luke.

Who's responsible for combating Internet fraud?

Share and share alike

"Everyone's got some responsibility. Ours is to ensure we give the right range of tools to our customers so they have all they need to fight fraud. The owners of the website have a responsibility to select a payment gateway that is PCI-compliant and also to educate their customers about how to use their cards safely. The banks have a responsibility, and the likes of Visa and Mastercard have schemes like 3D Secure to secure transactions. "

Joe Robey, head of business development, Sage Pay

Commercial question

"As an American, I believe my card or payment mechanism is 100 per cent risk free to me. So if my card details are stolen, I am not liable in any way, shape or form, and any fraudulent transaction will be refunded. For US cardholders that's the way it works: the burden should be on the commercial side. There should be some best practices for the payment providers and the vendors, because they have a lot to lose. But this is also an opportunity for card issuers and vendors to improve the trust fabric with things like the green bar and locked padlock icon."

Phil D'Angio, director, VeriSign

The weakest link

"People like to point fingers, but the answer has to be everyone, because fraudsters target the weak points. From the end user sitting at their computer all the way down the chain, there are intermediaries, merchants and banks. Each step along the way is a potential point of vulnerability. The customer has to bear responsibility, and have antivirus and use websites responsibly. The merchants have to have a safe website if they are holding customer details."

Gareth Griffith, head of risk management UK and Ireland, PayPal

behind the scenes. Some of them are a real eye-opener.

The basic level of fraud screening they offer uses the address verification system (AVS), and CV2 number – the three digit code on the back of a credit and debit card. The aim here is to combat Cardholder Not Present fraud by allowing the issuing and acquiring banks to check the customer out.

The next level of fraud checking involves automated transaction monitoring. For example, PayPal checks each of the $2,300 worth of transactions a second that go through its system, says Garreth Griffith, head of risk management at PayPal UK and Ireland.

"We spend millions on this stuff, to monitor every single transaction, and we have ridiculously complex systems to do it," says Griffith.

In 2008, PayPal acquired Fraud Sciences for $169m. The Tel Aviv firm was a specialist in looking at minimal information on a customer to work out whether they were good or evil.

PayPal has now integrated Fraud Sciences' risk tools into the fraud management system it uses to monitor all transactions.

Fraud management systems work by scoring individuals using a traffic light system. Purchases who give mobile phone numbers and web email addresses as their point of contact score lower than people who give their home account and landline, for example.

But fraud systems also look at many other variables, says Griffith. Some of these may be a surprise. For example, they might also log the machine's IP address as well as the time of the transaction and the speed of the keystrokes.

This is mainly to work out whether the transaction is being requested by a human or a software algorithm belonging to a cyber criminal. "A machine acts different from a human, and we need to be able to pick that up. Pattern recognition technologies are absolutely fundamental," says Griffiths.

POLICING THE WEB

Behavioural analysis is becoming more sophisticated and has a more in common with advanced policing than ever before. Analysis experts are employed by the likes of PayPal and Sage Pay, and the major banks, and also fraud management services like The 3rd Man, which can offer another layer of checks.

These specialists are skilled at going through individual transactions to spot risky transactions and irregularities, and root out cyber crime.

The organisations mentioned also collect as much information as they can about the cardholder, and have been doing for some time, which probably should be a civil liberties concern. As a result, they have built up vast databases that can alert them to blacklisted individuals and addresses, or email addresses that are linked to fraud.

Meanwhile, e-tailers can combat fraud themselves with more and better security at their disposal than ever before, says Phil D'Angio, director of business development at VeriSign. The technology firm provides encryption and authentication technologies for major banking websites and retailers.

He says that security icons, such as the locked padlock or `green authentication bars', help to give confidence to consumers, whilst reducing the risk of fraud.

VeriSign offers SSL encryption to scramble transactions or private details that pass through a website, and a service called VeriSign Identity Protection (VIP) to help protect account details through two factor authentication.

"SSL lets people know that the website is the one it claims to be. It also encrypts a web session so it's near impossible to snoop. Any serious e-commerce provider uses this sort of technology," says D'Angio.

According to industry experts, web security is set to become even more multi-layered going forward. Eventually it will incorporate military-strength encryption as well as biometric elements like fingerprint and retina scanning and voice recognition.

So far, current fraud management and security strategies seem to be working. Recent statistics have shown falls in Cardholder Not Present fraud.

But e-tailors are warned to remain vigilant because cybercriminals are inventive and relentless, always looking for the next weak point in the system. "If a door shuts somewhere, people will always find the next open door," says Sage Pay's Robey. ■