

FINANCIAL TIMES

WEDNESDAY SEPTEMBER 19 2007

Digital Business | Management & People

E-commerce needs better authentication strategies

Security Matters

ANDREA KLEIN

While the global community goes about its daily business, a sinister force – the e-criminal – lurks as close as a web browser, threatening to stop e-commerce in its tracks.

Business and consumers have capitalised on the convenience and cost-effectiveness of trading online, but it could come to a crashing halt if companies and their banks stop insuring losses because of online fraud – as some have hinted they might.

The assurance that both parties in a transaction are secure is essential to thwarting rampant fraud, which places identity authentication at the heart of the battle for the future of e-commerce.

While e-criminals' tactics have evolved, many corporations have not responded in kind, at least when it comes to identity authentication strategies.

Times are a-changing. As businesses face critical decisions about whether or how to insure losses that result from e-crime, many are focusing on reducing their risk outright by fortifying the role of identity authentication. They are taking an end-to-end approach in partnership with their financial institutions.

Corporations and their financial institutions through the years have implemented countless security measures to address identity issues, but generally have pursued a piecemeal versus an enterprise approach. Many have learned

the hard way that relying on a series of discrete point solutions cannot provide end-to-end visibility or address the total threat.

For example, two-factor authentication, a frequently deployed identity authentication method that couples a password with another type of identification, has proved to be fallible – when used alone – at thwarting man-in-the-middle attacks, when a hacker intercepts confidential messages, using the information to access accounts.

When the link between the user and their internet service provider is phished or hacked into, the hacker can insert fraudulent sites into the workflow, collect password and personal information and use that information to access accounts or commit other identity fraud crimes.

The piecemeal approach falls short because most point solutions focus on access versus authentication. Thus, as long as an individual has the appropriate Pin/password or token combined with a user name or site key, he/she can gain access to a site or data.

This approach is short-sighted because companies need to understand and vet the way in which credentials are granted before they can rely upon them.

Solutions that simply authenticate a user's credentials, and not who the user really is – while noble first attempts – do not guarantee a trusted infrastructure, and only meet basic compliance with domestic and international identity

authentication guidelines and regulations.

To provide security of the highest level possible, organisations must perform multi-factor authentication across the enterprise, using a single comprehensive solution that integrates various point solutions for all-round protection; cross-authenticates the user with the site; and secures the two through digital certificates, which have been issued only after the parties have been fully vetted.

It is also critical to validate certificates against a real-time updated list that indicates whether or not the certificate has expired or been revoked.

Global interoperability of identity authentication solutions is another serious concern. Enterprises need authentication protection across international borders and a legal framework that is acceptable domestically and internationally.

Otherwise, a corporation or its financial institution could face the prospect of adjudicating disputes in jurisdictions around the world should a security breach arise or a digitally signed document not be accepted as binding – an expensive and cumbersome prospect.

Financial institutions have a unique role and opportunity in an end-to-end infrastructure that incorporates digital certificates as the identity authentication vehicle. They can leverage their position as a trusted third-party in the traditional off-line world and offer new services as a third-party issuer of online digital certificates, simplifying

the delivery for customers and eliminating the need to expand the number of parties trusted with personal and confidential information.

For corporates, the benefits of an end-to-end identity authentication infrastructure extend far beyond protection from cyber criminals. They can drive new revenue opportunities and operational efficiencies.

Corporations using an end-to-end approach can rely on the authenticity of digital signatures for purchase orders, invoices, compliance, and other documents, allowing them to automate – finally – the last legs of the financial supply chain.

Businesses are optimistic about the potential of comprehensive identity authentication solutions to help them capture new business opportunities.

A recent Economist Intelligence Unit survey of business executives revealed that 45 per cent of the 246 respondents said that effective identity authentication would enable their businesses to grow more rapidly over the next three years.

Two-thirds said identity authentication was a priority for their companies because it could deliver business benefits, such as expediting receipts, as well as strategic benefits, such as facilitating entry into new markets.

Most consumers will not share their bank account passwords over the phone with a caller claiming to represent their bank, but many financial institutions and consumers adopt reckless privacy

practices when doing business online. In the rush to expand their online storefronts, many organisations have focused on ease of use while relegating security to an afterthought – leaving the institutions and their customers vulnerable to financial losses and critical damage to their reputations.

A strong online identity authentication strategy, however, does not require businesses to sacrifice ease-of-use or replace their current data security infrastructures.

Rather, companies taking the leap from a point solution to an enterprise approach stand to gain unprecedented levels of assurance for their e-commerce initiatives as well as new opportunities for efficiency and expansion – a win on both the offensive and defensive fronts.

Andrea Klein is chief marketing officer for IdenTrust, the global identity solutions provider.

Why online shoppers need an education

The rise of card-not-present (CNP) fraud, where purchases are made by credit card over the telephone or internet, rather than face-to-face, is having an impact on consumer confidence, writes **Kieron Guilfoyle**.

A study into the UK's e-commerce industry by the Office of Fair Trading showed 79 per cent of people are nervous about putting their card details online. Should CNP fraud continue to grow unchecked, the number of people using the internet to get the best prices may dwindle.

Similarly, as a growing number of businesses use the web to search for cheaper suppliers, they too may show increasing reluctance to trade online.

As a response, online retailers need to put more resources into communicating the message of secure shopping to their customers, be they individuals or businesses.

Their message is clearly not getting through. The idea is not to create a culture of fear – no action should be taken that impacts negatively on the “customer journey” from arriving at a site to transaction completion – but to reassure customers that the site is secure, and supports the use of safe shopping products.

One feature that could be highlighted is the padlock. The OFT study showed that while people recognise the padlock symbol on a website as a positive sign, many were still confused by what it signifies.

Retailers should reassure customers by drawing attention to the symbol and telling them that it means their card details will be transferred securely. That way, consumers know they are shopping at their own risk if the padlock is not present.

High profile cases in which payment card details are stolen

also offer an opportunity for retailers to remind customers that they store card details securely, in compliance with industry standards.

If shoppers remain unconvinced that their card details will be both transferred and stored safely, there are extra measures that retailers can use. The payments industry has introduced products such as Verified by Visa, a password-protected identity-checking service which provides strong security. Some products, such as our own pre-pay 3V Vouchers, even remove the need for consumers to put their card details online altogether.

Telling the public about these systems can only serve to heighten confidence and ensure customers do not take unnecessary risks.

Kieron Guilfoyle is CEO, 3V Transaction Services