



## TECHNICAL BRIEFING

October 2008

# Behind the mask

*Brett Feldon, general manager, EMEA, at VeCommerce, considers the extent of financial crime & how banks can arm themselves against fraud*

**F**igures released in July by APACS, the UK payments association, show that the number of adults using online banking has increased by 505% in the past seven years from less than 3.5 million in 2000 to just over 21 million last year. At the same time, Internet-based financial crime is also on the up with techniques such as phishing and spyware scams increasing at an alarming rate. There were more than 20,000 reported phishing incidents in the first half of 2008 – a jump of 180% compared with last year, making both banks and their customers more vulnerable. So what are the real risks and ramifications that financial institutions face, what can be done to fight crime, and what technology is out there to help?

### Origins of risk

Assessing and understanding both the types and origins of risk is the starting point for formulating a successful strategy to fight fraud. So who is behind today's financial crime and what forms does it take? Fortunately due to the successful introduction of campaigns such as Chip and PIN, face-to-face crime has dropped steeply, but as a result 'softer' targets such as CNP (card not present) fraud have become the new playground for criminals. The different types of on-line fraud have become increasingly sophisticated and the scale at which phishing, spyware and vishing operate has also shot up. For example there were 25,797 phishing websites targeted against UK banks and building societies in 2007, compared with 14,156 in 2006.

And it's not just organised crime that banks should be worried about. Internal fraud has also proved to be a problem – think about the actions of rogue trader Jerome Kerviel and the consequent fallout at Société Générale or the former employee at HBOS who managed to commit £21 million fraud based on fake loan accounts, before being detected. These cases have been well-publicised and the majority of banks already know how and where fraud comes from. What is less clear however is how and with what methods they should attempt to curb this crime. Should banks rely more heavily on technology to close the loopholes or do they need to go back to first principles and make more fundamental changes to the way in which financial transactions are actually authorised in the first place?

### Identity is key

Over the last twelve months, many of the UK's banks have introduced card readers for either some or all of those customers that enjoy on-line banking, a figure that now equates to over half of the UK's internet users. The motivation behind these devices was to improve security for customers by introducing two factor authentication, and therefore reduce the chances of someone assuming someone else's identity.

Whether the criminal attempts to steal personal information through phishing or they manage to access this information as a customer representative within a bank's call centre, the card readers introduced another identifier that

was believed to be difficult for fraudsters to get hold of. The idea behind the readers was a sound one, but unfortunately in practice they have a number of drawbacks. Firstly, the readers were very unpopular (look at any associated on-line consumer forum and you will soon see the depth of bad feeling) mostly because they either lost them, they couldn't remember their passwords or they did not always carry the devices with them.

What the banks failed to appreciate was that, yes their customers were keen for extra security, but they also wanted convenience: they did not want the hassle of carrying around an additional piece of equipment. On-line banking, after all, is about offering the customer anytime, anywhere banking. The other major flaw, of course, for these devices is the possibility that they can also be stolen, or used by someone known to the account holder.

### Is it really you?

At least what has been recognised by the industry as a whole is the importance of introducing better ways of identifying that an account holder is who they say they are. By addressing this key point, it is possible to prevent fraud. Think back over the last 12 months and the number of highly publicised data loss incidents. Naturally the media have criticised those that have been responsible for the lapses in security and have highlighted the dangers of personal details falling into the wrong hands. However, the impact of these would be less serious if it wasn't for the fact that too much emphasis is placed on the use of personal details to authorise transactions. Take for example the latest scam of 'vishing' which is used to fraudulently obtain sensitive data via the phone. With the rise of VoIP-based telephony it is easier to disguise where you are calling from and therefore easier to fool someone that you are calling from their bank. By requesting the victim to then call back and confirm security details via an automated system they can capture all the information they then need to commit fraud. But imagine if a bank was to insist on a form of identification that could not be stolen, replicated or 'borrowed'?

### The case for biometrics

This is why voice biometrics technology is finally being reviewed by the financial world as a practical and reliable means of solving identity verification. At present, the basis of most fraud (including the likes of 'vishing' and 'phishing') is reliant on extracting and then exploiting the personal data. The benefit of introducing voice biometrics is that a user registers their own unique voiceprint and for subsequent transactions must supply their voiceprint to gain authorisation. The beauty of the system is that no one can steal your voice and tests have shown that even mimics fail to fool the system. Other biometrics such as fingerprint or iris scan are also being widely used for unequivocal identification, but unlike voice, both of these rely on the person being present. The lion's share of fraud now takes place when the card holder is not present, which makes both →



## TECHNICAL BRIEFING

October 2008

of these less viable. What's more, a voice biometrics solution does not need any additional equipment such as a reader – it can all be done over a normal telephone.

### How it works in practice?

A typical scenario using voice biometrics might involve a customer that wants to make a transfer using an on-line account. After signing onto the banking website, the customer makes a transfer request and the system would then apply appropriate rules to decide whether additional validation is required. If so, an outbound call is placed to the customer. The call confirms the account/payment details and authenticates the caller using the registered biometric voiceprint. The web server is then informed of the authentication outcome and the transaction is processed or denied dependent on whether there is a match. A confirmation is then sent to the customer via email. The use of a separate channel for part of the authentication process eliminates some types of attacks on the internet banking system.

Once enrolled, the caller's identity can be verified quickly and simply without ever having to provide their personal data again, although for additional security it's likely the caller will be asked for a combination of voice print *and* personal details. It often takes a call centre 40 seconds less to verify a caller's identity using voice biometrics than it does using traditional means, so not only can banks improve service and security for customers but they can also reduce their operational costs.

### Tackling internal fraud

This same technology can also be applied to address internal fraud especially amongst call centre staff. In the past, many staff have had access to personal information, but with the use of technology such as voice biometrics and/or automated voice systems such as interactive voice response, agents no longer need to be privy to this information. The FSA has made its position clear on banks' responsibilities. FSA financial crime sector leader Philip Robinson said: "It is up to individual firms to decide how to manage the risk of insider fraud. However, examples of good practice found in the industry including good vetting of staff, segregation of duties and IT controls to prevent access to systems or data that could be used to commit fraud." Banks that fail to heed warnings will not only have to bear the costs of fraud themselves but also risk hefty fines: in May the FSA fined BNP Paribas Private Bank £350,000 for weaknesses in systems and controls that let an employee transfer £14 million from clients' accounts.

At a point when the World's banking community is facing turbulent times, there are now even greater reasons to reassure and build confidence amongst customers. With the new ISO 19092:2008, Financial Services – Biometrics – Security framework published earlier this year, banks now have some global standards to work with. There is now a perfect opportunity for banks to differentiate themselves in their ability to tackle financial crime – the question is whether they choose to take it.

[www.vecommerce.co.uk](http://www.vecommerce.co.uk)