FStech

# Security sentiment

The results of the *FStech* Security Sentiment Survey in retail banking make for interesting reading. If you thought all security professionals think the same, then read on...

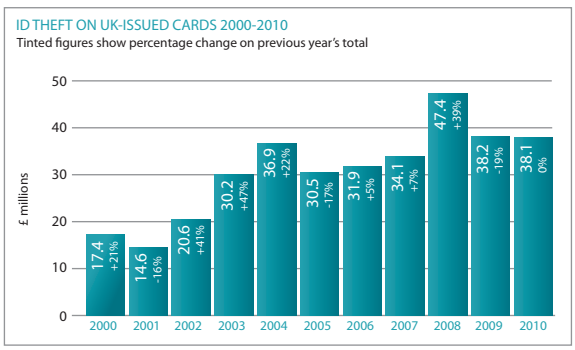
## INTRODUCTION

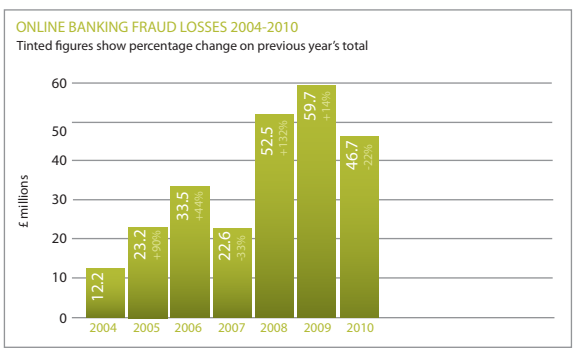
The term security consistently gets a reaction from anyone in retail banking. To some extent the concept of security is what defines a bank – a safe place – but advances in technology have created assets that are increasingly difficult to protect.

In addition, customers' desire to use technology, such as mobile banking, attracts increasingly sophisticated attacks, and it means that the CISO has to be aware of not just what is happening, but what is likely to happen in the future.

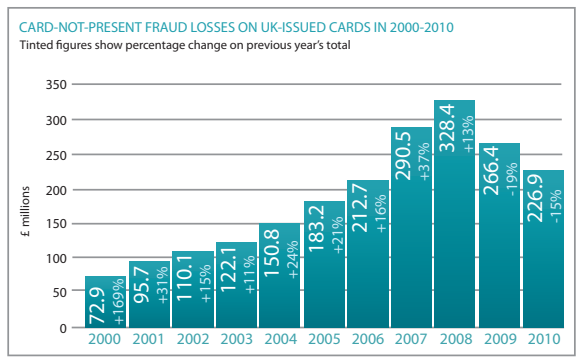
## BACKGROUND

To put this into context, fraud has risen consistently over the period of 2000-2008. After this period fraud has, in monetary terms, declined slightly. It might be premature to wave a victory banner however:




*FStech* magazine surveyed over 100 CISOs and heads of security to gain insight into how the security community sees the issues changing and how they, the professionals, feel that security can be improved.




Figures from the Financial Fraud Action UK

Whilst some progress may be down to improved security, such as card readers, there are other factors that could contribute to this fall, the largest of which are the economic conditions we find ourselves in. Reduced spending and reduced lending make fraud harder to commit. And as the economy recovers it will be interesting to see how the figures change, especially in light of the next phase of mobile devices that consumers will be using.

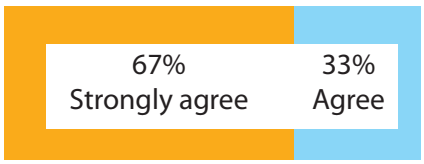
## THE SENTIMENT SURVEY

*FStech* surveyed over 100 security professionals in UK-based financial institutions over the autumn of 2011, during which time there were several data breaches (the ICO reporting a 58% increase in the year within the private sector). These included data stolen from third parties, Sony most notably.

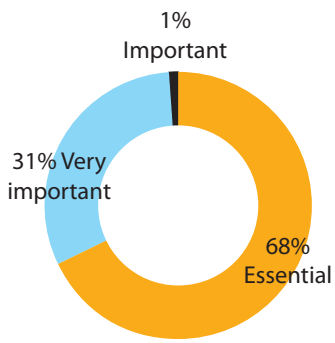
## RESPONSIBILITIES

How do banks see their responsibilities? From the CISO's point of view, protection of assets (in this case data) is a central task, but protection of the consumer whilst shopping online is a bit further from their perceived remit.

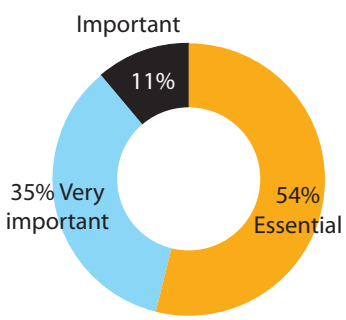
Asked how high a priority tackling card-related fraud is, the following results were recorded:




Clearly, the financial institutions themselves see the reduction of fraud as very important, and there is a desire to create better security. This can be ascribed to a number of reasons, including customer relations, as detailed by the question of ranking the importance of protecting customer data, where 68% said that it was essential.



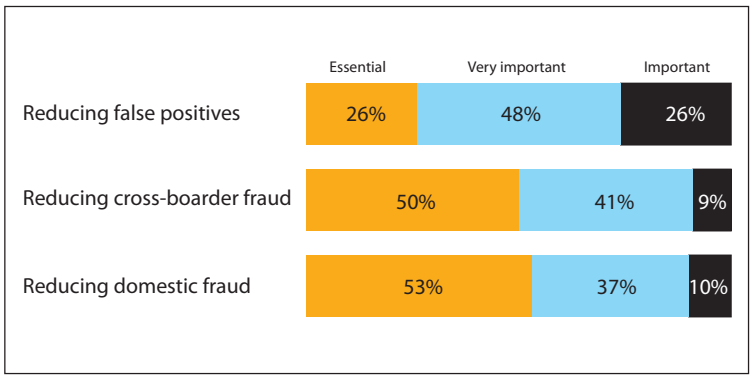

But then, asked whether it was important to enable customers to shop online securely, the results were:




The sentiment expressed might not mean that banks fail to pursue technologies that reduce fraud, but it does imply that there is slightly less emphasis on securing the whole transaction process with retailers than there is to secure data. One cannot help but wonder if regulation and fines for breaches has done something to focus the minds of the banks on the immediate and direct concerns of security.

## PRIORITIES IN REDUCING FRAUD

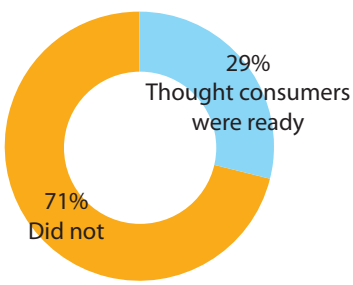
We asked about reducing fraud and the priorities that the respondents felt their organisations placed on each type. These were:




The desire to reduce domestic and foreign fraud are of course both understandable, and are clearly seen as almost equally important. False positives, on the other hand, are seen as a lower priority, perhaps because a false positive means that there is no fraud committed, but it might also be read, in conjunction with the above result on protection of online shopping, as less of a worry because there is less of a penalty for the bank, or less emphasis on the customer experience.

## THE MOBILE WALLET

So what will the respondents make of technology that bridges the gap between the bank and the retailer? The mobile wallet has been talked about for some time, but now it is a reality, and we asked how ready the average UK consumer would be to embrace this technology over the next year.




The high numbers of doubters may be holding memories of the take up of contactless payment – which has been less than desired

or predicted, but the mobile wallet might be a different story. For a start, the UK has a mobile phone penetration rate of over 100% (130.6% ITU 2009) and contactless payment is now far more common (for example, with contactless payment and Oyster cards in London). The tipping point may arrive far faster this time around, but we shall see.

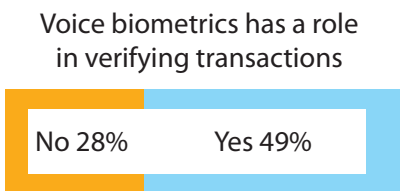
Slow take up could be for a number of reasons, but interestingly our respondents placed security as a major hurdle. If this is true, then better security presents an opportunity to help pave the way for the technology. Asked the factors most likely to prevent UK consumers from embracing the mobile wallet over the next year, 47% of respondent said security. The next highest identified barrier was the lack of point of sale opportunities.

## MOBILE MATTERS

The mobile phone is becoming the essential item of the modern world, and the mobile wallet is one extension of that. But even at the level of being the communication device between the customer and his or her bank it has taken significant strides forward, and intelligence organisation Datamonitor envisages UK use not only accelerating to match global uptake, but also to overtake internet as the main way for consumers to bank. We asked the banks if m-banking has the potential to increase or decrease fraud, with a majority of 63% saying that it can decrease fraud.

So the phone is seen as a way to help secure transactions, but another issue that clearly worries our respondents is the issue of SIM-swapping in mobiles – with 67% expressing fears over the ease of this procedure.

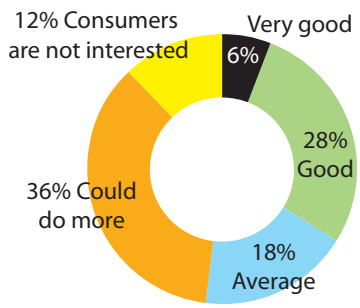
In addition we asked if voice biometrics also has a role to play in that tighter security, in part with mobile:




Perhaps, and at long last, biometrics will start to have a role in banking. Again this might well be a case of finding the tipping point between customers' annoyance with new systems and fear over their security (and interruption to use of banking facilities).

## THE CUSTOMER

If you reverse the question, and ask the industry how they feel the public views their efforts to reduce fraud, you get a rather surprising response:




One might think that the response is somewhat fragmented, with some believing the public have a lot of confidence in security, others feeling the public could not care less. Whilst there is probably truth in both – after all the 'public' are not all going to agree – the results show a majority who believe that security could be better and that the public perceive this to be the case.

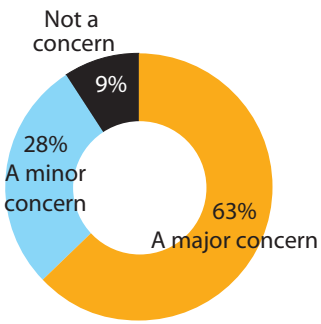
To go further is speculation, but it is likely that our respondents are aware of the constraints that the public has placed on them, such as not being willing to use complex verification processes, whilst still wanting to feel secure. Whilst the public might feel secure in some cases, this might well be a misplaced sense of security, as 82% of respondents believe that customers do not fully appreciate the risks presented by card not present fraud.

Along similar lines, a 94% majority believe that the public is unfamiliar with fraud operations and terms such as 'man in the browser'. So, certainly there is evidence that the industry could do more to help reassure customers, and a separate question on phishing generated a response of 74% supporting the idea that greater protection on this issue would generate more confidence among the public, there is also the sense that the public are not sufficiently educated to the risks to make decisions on security – such as choosing an account with high security.

This might be changing however, due to the greater coverage that data breaches and card fraud are generating. Roughly half of the respondents believe that customers choose an account in part because of the level of fraud protection, and half do not. And there is a similar split on the adverse affect of having a card declined at an ATM, online or in a shop.

### THE THIRD MAN

Banks, building societies and other financial institutions are aware of the security threat, and they are aware that legislation on areas such as data breach is only likely to get tougher. However, there are elements that are beyond their control, and these include the personal and account details that are stored by third parties. Asked if information collected indirectly and then breached, such as recently occurred with the Sony Playstation, was of concern, the results were:




Which places the threat form outside sources squarely in the major league with a combined 91% concerned. Again, one might suggest that protection of the data is something that might be impossible to do when so many details are required and stored online, but protection of the transaction might be a reasonable and realistic opportunity to prevent the 'benefit' of fraud.

### SUMMARY

In summary we can say that security is a major priority and one that will vex the CISO of every organisation. With raising awareness in consumers, and financial institutions who see fraud protection as part of the offering to the public (and, after all, if you were a bank wouldn't you rather appeal to the security conscious customer?) the converging forces can, however, result in stronger barriers to fraud.

What we can also say is that there will be more creative and more effective anti-fraud technology to combat the fraudsters. It is a battle that is unlikely to end any time soon, but one where, just perhaps, technology is helping to turn the tide.

### WHAT DO THE BANKERS SAY?

As previously noted, the survey is, by its nature, an average of views, so we decided to place the results in front of a few selected individuals in the industry, and get their feedback. All three reinforce the idea that it is consumer confidence in security that is of vital importance for the further progress of payments.

"What struck me was the disconnect between the 47% of respondents who believed that the biggest factor likely to prevent use of mobile wallets was security and the 63% of banks who thought that m-banking had the potential to reduce fraud. If the industry can effectively communicate the security advantages of mobile banking services, there is an excellent chance that mobile banking can be the success that contactless payments have not."
*A representative of an Anglo-Amercian bank.*

It is important that as the mobile wallet and contactless payment gather momentum, both banks and the general public move forward together. Fraudsters have always been quick to respond to opportunities that new technologies present, so banks need to let the public know what these new risks are.
*A large UK retail bank*

"Online security and fraud prevention are probably the most important topics for banks to keep addressing if they want to see their electronic channels continue to grow. The benefits of this continued growth are manifold and continued investment will continue to be very worthwhile."
*A major international bank*

In summary, the message is clear – security is a significant issue for the wide spread adoption of electronic payment, and yet is seldom seen as a potential selling point or area where convenience can be created. Perhaps the banks are missing a trick?