

## Who Are You?

**Identity fraud costs UK PLC £1.3bn a year and with the threat set to grow, it could become the single biggest transparency challenge for marketing and communications.**

It was supposed to be a promised land.

The internet would bring new efficiencies and increased levels of service to practically every industry sector and every public sector organisation - a new, convenient way to conduct practically any transaction.

There was just one issue – the security. Sure, you could encrypt messages. But how would you authenticate users? Well, get them to authenticate themselves with a combination of passwords and usernames. It was an imperfect solution, but for a while it seemed enough.

Now the cracks are beginning to show.

Steal someone's identity and you can get access, not just to the money in their account, but to every line of credit they have – and anything else anyone is willing to offer them.

As a criminal, your challenge is to get hold of personal details and passwords. And the techniques for collecting these is becoming ever more imaginative and easily available – free do-it-yourself phishing kits have been published for download on the web, for example, and new scams seem to come to light on a weekly basis.

Although the banks are the immediate focus, ID theft could feasibly become a real issue for any organisation that routinely collects and stores personal information – or uses the internet to conduct transactions.

The banks and others, including Government, are making serious and sustained efforts to deal with this issue at a number of levels. But as personal identity becomes no more than a set of bytes in an inter-linked mesh of computers, identity fraud is creating new challenges for corporate communication professionals.

What are these?

- **Scale**  
Identity fraud is growing and going to be with us for a long time to come. As it becomes more frequent and affects more companies and individuals, it will become an even bigger area of investigation by media, consumer groups and even the political community. The need for organisations to explain and possibly even report their policies and procedures will increase.
- **New situations**  
Identity fraud is evolving fast thereby creating new risks and new types of 'incident'. Anticipating and mapping these incidents and integrating them into a company's existing issues and crisis communication plans will be critical, especially to those not yet versed in the threats.

- **Knowledge**  
The technology which defends and attacks business is constantly evolving. Understanding the nuances, and explaining them to media, analysts and other audiences will require communications professionals to update their IT knowledge and messaging constantly. To complicate matters further, many companies will want to keep their countermeasures private – so how exactly do they do this without appearing evasive?
- **New liabilities**  
Identity fraud may create new legal ambiguities and, in the future, the burden of liability between different companies and consumers may change. For example, when a digital ID is stolen via one organisation and the used to defraud another, where exactly does the liability lie? Again, understanding these changes and ensuring communications is up to speed with them is critical.
- **New customer experiences**  
Home Office research shows ID fraud can take up to 300 hours to clear up – during which time customers may be turned from loyal advocates into brand critics. If this figure is true and the number of incidents expands, the communication team could be facing a significant increase in media investigations supported by angry and disappointed customers who feel they are being treated appallingly.
- **The 'smell of blood'**  
Given the personally invasive nature of the crime, it is always going to be newsworthy – high-tech methods, perpetrated by highly organised, extremely audacious criminal gangs, operating in exotic locations makes great copy. Our own research suggests media already feel they are not being told 'the whole story' and this will make them more suspicious and more inquiring.
- **Trust and belief**  
ID fraud has the power to change consumers' belief, behaviour and trust. Among victims of online identify theft the effect is even more marked - Forrester Research confirms they become far more wary of any type of online transaction. Similarly, research by Visa in the UK demonstrates that, when someone becomes a victim of card fraud, there is invariably a marked change in their subsequent spending patterns. Managing this is a strategic issues management challenge in which the whole organisation needs to engage – bur one in which marketing and communications has specific responsibilities. Will it be the companies which actively and transparently educate stakeholders about the issues which win or those who hide?
- **Treatments vs. Cures**  
Many different technical solutions are being proposed by many different advocates. Each of these has its own merits, but none can be regarded as a panacea. ID theft methods are incredibly quick to evolve and mutate and – faced by new technical barriers – could become ever more audacious and invasive.

How you view ID fraud will always be determined by your own particular goals and vulnerabilities.

You may look at the threat simply as a *short term crisis management issue* (a set of specific incidents to be anticipated and responded to as and when) or you may regard it as a *long term reputation management issue* (how are you going to maintain consumer trust in the efficacy of your on-line services).

Many companies will need to do both.

In many different ways the internet-related predictions of the 1990s boom years are now coming true. It was envisaged that swathes of the world economy would move online. It was also envisaged that the criminals would follow suit.

This new reality means companies must review their crisis and issues policies and procedures and educate their communications people more fully, so they are sufficiently versed in the realities and implications of this threat to be able to manage and defend their organisation's greatest intangible asset – their reputations.