



25<sup>th</sup> January 2006

## PRESS RELEASE

### Tricerion Protects Online Bank Customers from Compromising Login Details

Tricerion Limited's innovative online authentication technology doesn't just protect online banking customers from fraudsters – it protects customers from themselves.

The UK Financial Services Authority's *Financial Risk Outlook Report 2006* (published today) highlights the fragility of consumer confidence in online banking security. The FSA report concludes that "banks should continue to drive security and this must include educating consumers on the importance of protecting themselves."

Tricerion believes that security solutions that are forced to rely on consumer education in order to remain secure should not be considered secure. Human error is a fact, and secure solutions must manage it securely. Consumers need solutions that make it easy and intuitive to act securely at all times, while rendering it effectively impossible for them to compromise their own or the system's security. These principles are embodied in Surrey-based Tricerion Limited's Secure Mutual Authentication (SMA) server.

The Tricerion SMA server is installed inside the banking institution's firewall, alongside the online banking webserver. Users log in by entering their user name, and are then asked to enter their password by clicking symbols on a keypad. The keypad look-and-feel is personalized to each user, so alert users may notice the lack of such personalization if they are directed to a fake web site during a *phishing* attack. However, the security of the system does not depend on the user noticing the presence or absence of such clues. Personalization goes beyond this to the extent of presenting each user with an individual set of input symbols, drawn from a very large set of available symbols. Users can only enter their password – consisting of a sequence of picture symbols – from their own personal input keypad.

Even if users fail to notice that they are being phished, they *cannot* disclose their password unless presented with their own personal input keypad – information which is not available to phishers. Neither can they disclose their password by describing its picture sequence, since there are many conceptually identical but graphically distinct symbols in the available inventory. Reference to a symbol's position in the keypad (e.g. "top left") is useless since the symbol positions are scrambled on each presentation. Picture passwords drawn from personal symbol inventories are remarkably difficult to disclose to anyone, without access to the appropriate personal keypad.

Picture passwords nonetheless prove to be highly usable for legitimate users, and tend to be remembered more reliably than conventional passwords or PINs. This is related to a finding of experimental psychology known as the *picture superiority effect*. First demonstrated almost half a century ago, and frequently tested since then, the picture superiority effect is a tendency for people to recall pictorial information more reliably than textual information. This is thought to be because different parts of the brain are used in the process. Pictorial information is *recognized*, whereas textual information must be *remembered*.

Once issued with pictorial passwords users need no instruction in the use of input keypads to understand how to login. All users so far tested have intuitively known how to proceed.

Tricerion's SMA solution is an example of what is sometimes called *mutual authentication*. In conventional logins the bank requires users to authenticate themselves to the bank before they are allowed access to their account. In mutual authentication, the bank also has to authenticate itself to the user to prove that it is the real institution and not a phishing site. In effect, users say, "I will only tell you my secret password, if you first tell me a secret that only you could know." Some mutual authentication solutions present users with pre-selected pictures or look-and-feel elements to 'prove' the institution's identity. But these rely on the alertness of the user to notice that something is amiss. Such approaches do not prevent users from proceeding if they fail to notice, or do not understand the significance of what they see.

Tricerion's key innovation is to make the bank's secret information – the user's personal keypad – crucial to the viability of the authentication event. Unless the bank reveals its secret, the user *cannot* reveal theirs.

The ineffectiveness of security approaches that rely on user education can be seen in recent trends in online fraud. In the year and a half after phishing first appeared in late 2003, most attacks relied on social engineering, i.e. creating good fake emails and web sites that fooled users into disclosing their login credentials. More recently, according to the Anti-Phishing Working Group, there has been a dramatic rise in recorded attacks based on Trojan viruses, rather than social engineering. Some of these Trojans log keystrokes, including login credentials, and post them back to the fraudsters. Tricerion picture passwords are never typed so there are no keystrokes to capture, and thus security is preserved. Other Trojans capture and post screenshots when mouse clicks occur. Tricerion's 'active countermeasures' are able to combat such attacks and ensure that captured screenshots contain no useful information.

Dr Norman Fraser, Chief Executive of Tricerion Limited comments, "Unlike authentication solutions based on physical devices (such as password tokens or biometric readers) or on software installations, Tricerion's SMA solution achieves the holy grail of delivering highly usable, two-factor, strong authentication with a 'zero footprint', i.e. with no ongoing logistical overhead. This makes it the cheapest high security solution to roll out to large populations of users, while its resilience to human error and its extreme usability remove the need for investment in a supporting user education programme."

### **About Tricerion**

Tricerion Limited was founded in England in 2004 by a group of experienced British inventors and technology entrepreneurs. Its patent-pending identity authentication innovations form the basis of its Tricerion SMA server. The company signed its first banking customer in 2005. Tricerion's Atlanta office is actively working with US financial institutions as they seek to meet recently published Federal guidelines requiring the implementation of strong authentication by the end of 2006. More details on Tricerion and its innovations can be found at [www.tricerion.com](http://www.tricerion.com).

For further information contact:

Dr Norman Fraser, Chief Executive  
Tricerion Ltd, 65 High Street, Egham, Surrey TW20 9EY, United Kingdom  
Email: [norman.fraser@tricerion.com](mailto:norman.fraser@tricerion.com)  
Tel: 07834 760766

### **Useful links**

Financial Services Authority - [www.fsa.gov.uk](http://www.fsa.gov.uk)  
Anti-Phishing Working Group - [www.antiphishing.org](http://www.antiphishing.org)