



[HOME](#) | [NEWS DESK](#) | [ARTICLES](#) | [WHITE PAPERS](#) | [VENDOR GUIDE](#) | [WRITERS](#) | [NEWSLETTER](#) | [ABOUT US](#)

Article appeared on April 7, 2004

Comment

Identity theft and fraud is more sophisticated than ever, and is set to cost financial institutions an estimated \$3.375 billion in 2004. Instead of attacking the financial institutions' security systems, thieves extract usernames, passwords, PINs, account numbers and other personal information from unsecured end-users. StrikeForce Technologies' new identity theft solution, COBAS, is an authentication system that verifies an online bank customer's identity through the customer's telephone.

Full Story

StrikeForce Technologies has released COBAS (Centralized Out-of-Band Authentication System), a solution designed to stop identity theft and fraud in the financial industry. COBAS is a clientless dual/tri-factor identity authentication system that utilizes 'out-of-band' technology. It never exposes an end-user's credentials, but rather creates a separate pathway for authenticating a user's credentials using devices like telephones, PDAs or instant messaging. Customers no longer have to input both their username and password at login - with COBAS the user inputs only their username. Their phone rings a few seconds later and they type in a passcode or, for an additional layer of security, the user can choose to be verified using voice recognition.

"Online security, consumer confidence and loyalty go hand in hand. When a bank provides a secure end-user solution to identity theft, customers are more comfortable doing business and increase their number of transactions," said George Waller, vice president of sales and marketing for StrikeForce. "COBAS not only improves the customers experience, it gives IT managers a flexible and robust solution that achieves higher levels of security at 25% to 50% of the cost."

In the COBAS model, a user's credentials (password, biometrics or layered combination) are routed over a private one-way outbound server, away from the client network and out of reach from hackers or intruders. According to StrikeForce, out-of-band authentication has proven to be more secure than other forms of security, where both the username and authentication data are packaged together and travel across the same network.

When a bank provides COBAS to authenticate its online customers, each online user registers a preference for the method by which he or she would like to be authenticated. Users have the option of receiving a telephone call or a secure instant message from a COBAS Identity Agent (CIA) housed on the user's computer. Biometric devices such as fingerprint, iris scanners and voice recognition can be added to the process for additional layers of security.

COBAS can also be applied to workflow or process authentication situations in which approvals have to be escalated up the chain of authority. For example, when a bank's employee authorization to perform a wire transfer exceeds their threshold amount, COBAS automatically performs another out-of-band authentication with an escalated second user to authorize the requested amount.

The company's out-of-network model integrates with current and emerging authentication products — biometrics, tokens and smart cards — and, tied with a password, achieves tri-factor authentication. Its out-of-band model adds a measure of security to all platforms — extending functionality and eliminating the need for costly middleware. Its 'client neutral' status enables it to layer all biometric devices over any combination of operating systems, including Microsoft, Linux, SUN, Unix, Novell or mainframe.