



**FOR IMMEDIATE RELEASE**

## **Breakthrough Identity Theft Weapon has link to “Cap’n Crunch”**

*StrikeForce’s Personal Agent Authenticates Identity each Time a Consumer’s Personal Information is Accessed*

**Edison, N.J. – October 08, 2003** – As consumers struggle to keep their personal information secure during online transactions, one e-security company, StrikeForce Technologies, Inc., is offering a new security platform. The technology traces its origins to the successful model the phone company used to stop hacking in the 1970s. In the same way that AT&T split the pathways that carried their voice and signaling data to stop phone phreaking 30 years ago, the new model takes the authentication step of security out-of-band -- splitting the physical pathways that carry usernames and authentication data.

The out-of-band methodology, known as COBAS (Centralized Out-of-Band Authentication System) is recognized as the world’s only universal authentication platform to solve the underlying fatal flaw of computer security – packaged credentials.

During the Phone Phreak movement, phone phreaks discovered that voice and phone signaling were being carried in the same band which led them to replicate certain tones and secure free long distance service. The leader of the movement, a Vietnam vet named John Draper was given the moniker “Cap’n Crunch” when he discovered that the giveaway whistle in Cap’n Crunch cereal boxes perfectly reproduced a 2600 Hertz tone needed to make free calls. To combat this early form of hacking, AT&T switched to out-of-band signaling, where the voice and tone signals are carried separately. This method proved effective virtually eliminating tone hacking overnight.

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

According to a study on identity theft by Privacy & American Business, 91% of consumers expect ID theft incidents to increase rather than decrease in the near future.

### **Identity Theft: A Closer Look**

- 27.3 million Americans have been victims of identity theft in the last five years, including 9.91 million people or 4.6% of the population in the last year alone.
- The emotional impact of identity theft has been found to parallel that of victims of violent crime.
- 92% of Americans think the government should take action on identity theft.
- There are over 71,000 websites dedicated to educating people how to hack.

“There are over 71,000 web sites dedicated to



educating the lay person how to hack,” said Ram Pemmaraju, Chief Technology Officer, StrikeForce. “As long as usernames and passwords continue to travel together, neatly packaged for hackers, we are making identity theft easy. By carrying username and password information separately, StrikeForce has leveled the playing field against hackers and thieves. With COBAS, it will not be difficult for hackers to steal someone’s identity –it will be impossible.”

### **How COBAS works.**

Using COBAS, each user’s transaction will be verified every time personal information is accessed. Suppose you are buying a pair of shoes online. When you go to check out, you will click to make a COBAS Secure™ transaction and will be asked to enter only your username. Within a couple of seconds of supplying a username, your telephone rings or an instant message pops up on your screen (depending upon which one you’ve registered). You’ll then be asked to use the telephone to key in your password to verify the purchase. The password, or pin number in this instance, is sent through the COBAS server, authenticated and accepted.

In the same way that your bank account is only accessible with specific ATM cards, this form of authentication only works on one phone---the phone that COBAS is programmed to call for you. Additional layers of security incorporating biometrics (voice recognition, fingerprint or Iris scanning) can be implemented to guarantee your identity.

Using COBAS Secure Transactions™ allows users to benefit from a 24-7 personal agent. Users are contacted by phone or instant message every time their information is used for an online transaction.

StrikeForce has licensed its COBAS product to Panasonic and myVirtualCard. It currently is in negotiation with several major credit card companies. COBAS can verify credentials in virtual private networks (VPNs), network logons (e.g.: a Windows domain) and in various forms of e-commerce transactions.

### ***About StrikeForce Technologies***

*StrikeForce Technologies is an identity solutions firm that has developed a revolutionary new security platform providing unprecedented levels of security, interoperability, and usability -- in seamless cost-effective designs.*

*The company’s award-winning distinction is a patent-pending technology, called COBAS. for (Centralized Out-of-Band Authentication Solution). COBAS creates a separate “out-of-band” pathway for authenticating a user’s credentials, away from the client network and out of reach from hackers. The open, out-of-band server allows easy integration and layering with today’s security devices (tokens, Smart Cards and biometrics) – and tied with a password, is the only product to achieve tri-factor authentication.*

*Headquartered in Edison, NJ, the company was established through the merger of Netlabs.com and Strike Force Technical Services, Inc. (SFT). Partnering with best-of-breed service providers and manufacturers, the company’s COBAS model is fast becoming the recognized standard authentication platform for today’s smart networks, access scenarios and enterprises.*

*For more information please visit [www.sftnj.com](http://www.sftnj.com).*