



**REDSPIN**  
SECURITY • COMPLIANCE • RISK MANAGEMENT

6440 Via Real, Suite 5, Carpinteria, CA 93013  
[www.redspin.com](http://www.redspin.com)  
805-684-6858

## FOR IMMEDIATE RELEASE

### **Bank Advisory from Redspin: The Real *Inside Man***

#### **Weak security and unencrypted data pose a threat to millions of ATM users, according to a new white paper from Redspin**

**Santa Barbara, CA, April 13, 2006** — Spike Lee's new release *Inside Man* tells the story of an intricately plotted bank robbery involving the ultimate "inside man." What many bankers around the country don't realize is that a digital inside man is hiding in their own computer networks right now.

"A number of bad scenarios can come out of this situation, the biggest being mass card number theft, like what just happened to Bank of America and Washington Mutual," says John Abraham, Redspin president. "Also, the wrong person with the right knowledge could become a 'man-in-the-middle.' They could spoof a processor's response to an ATM, telling it over and over again that the daily \$500 limit hasn't been reached. Back up the money truck."

Redspin, Inc. has released a white paper detailing the problem. Essentially, unencrypted ATM transaction data is floating around bank networks, and bank managers are completely unaware of it. The only data from an ATM transaction that is encrypted is the PIN number.

"We were in the middle of an audit, looking at network traffic, when there it was, plain as day. We were surprised. The bank manager was surprised. Pretty much everyone we talk to is surprised. The card number, the expiration date, the account balances and withdrawal amounts, they all go across the networks in cleartext, which is exactly what it sounds like – text that anyone can read," explained Abraham.

Ironically, the problem came about because of a mandated security improvement in ATMs. The original standard for ATM data encryption (DES) was becoming too easy to crack, so the standard was upgraded to Triple DES. Like any home improvement project, many ATM upgrades have snowballed to include a variety of other enhancements, including the use of transmission control protocol/Internet protocol (TCP/IP) – moving ATMs off their own dedicated lines, and on to the banks' networks.

More and more banks now run their ATMs through their own computer network before the information goes on to a centralized processor. While having the ATMs on the bank's network instead of a bunch of individual, dedicated lines is much more economical and much easier to manage, it greatly increases their security exposure.

The fact that ATM data isn't encrypted wasn't a problem when the information was going across dedicated lines, but now that it goes through the bank's Internet-connected system before going to a processor, it creates unexpected opportunities for crime and mischief. A hacker tapping into a bank's network would have complete access to every single ATM transaction going through the bank's ATMs.

"Our biggest concern is that not many bank managers know this," says Abraham. "They assume that everything is encrypted. It's not a terrible assumption, so it's no wonder that most bank managers we've talked to are unhappy to discover this after spending \$60,000 to upgrade an ATM.

"Fortunately," continues Abraham, "prevention isn't that complicated, as long as bankers are aware that there is a potential problem. ATM machines need to be kept separate from the rest of the bank's computer network, to try to recreate that direct line to the processor. Also, Redspin is developing a tool to help bankers determine their level of vulnerability. This white paper is all about raising awareness."

For additional information and a free copy of the white paper by Redspin's Brian Hayes, visit [www.redspin.com](http://www.redspin.com).

#### **About Redspin, Inc.**

Redspin is an independent auditor specializing in network security and compliance, providing objective IT [security auditing services](#) to financial institutions, casinos, e-commerce, ATM providers, Automated Clearing Houses (ACHs), utilities, and defense contractors. Redspin has performed penetration tests, FFIEC IT audits and other services for more than 100 banks and credit unions nationwide. For more information visit [www.redspin.com](http://www.redspin.com).

#### **Contact:**

Deb Montner, Montner & Associates, 203-226-9290, [dmontner@montner.com](mailto:dmontner@montner.com)