

MEDIA STATEMENT

PROTECTION NEEDED TO PREVENT CREDIT CARD FRAUD

9 June 2003

A West Australian company has the key to help prevent billions of dollars a year being stolen through credit card theft.

Earlier this year millions of Visa and Master Card members around the world were put at risk by a hacker accessing a third-party credit card processing system, accessing eight million accounts around the world.

Almost all cases of credit card theft occur when a hacker gains unauthorised access to an e-commerce site's server, and then is able to access the database that contains customer information.

When consumers swipe their credit cards at a checkout counter, their account number takes a long and winding path around a host of global networks that ultimately ensure the shop owner gets paid. During travel the credit card details are encrypted and it is usually safe until it reaches the destination.

Once at the final destination, the credit card clearing house, stores the details in a database on a server often unencrypted.

Chairman and Chief Executive Officer of Secure Systems Limited, Mike Wynne, said the reason most companies don't encrypt stored data was because they believed their firewalls would keep malicious hackers out and that encryption software would slow down the performance on the server.

Mr Wynne said his Perth-built Silicon Data Vault, (SDV®) was a hardware-based security device providing strong authentication, access control, and data protection through encrypting the entire hard disk drive (HDD), using sophisticated encryption key management.

Secure Systems Limited is developing an SDV which is operating system aware and would allow write only access to a secured database. If a malicious hacker tried to access the data, it would appear as though nothing was there.

Mr Wynne said there were two main perceived problems with software encryption products.

"Firstly they slow down the server and secondly the software can be manipulated to gain access to the key," he said.

"It might take 50 years to crack an encrypted message with a 512-bit key while it could only five minutes to hack into a system and steal the key which allows you to decrypt the message in seconds."

Mr Wynne said the SDV® was the first system in the world that combined hardware, encryption, and partition level access. There are four levels of access or denial to files within partitions; no access, read only access, write only access and read/write access.

The SDV also logs any unauthorised log-in attempts

"The SDV® is located in the Integrated Drive Electronics (IDE) cable and asserts absolute control of the hard disk drive during early boot, ensuring the user is authenticated before confidential files or data can be accessed," he said.

"Visa, MasterCard and American Express alone have more than 50 million customers at the mercy of computer hackers.

"Although zero-liability policies protect cardholders from paying for unauthorized or fraudulent charges, they don't protect consumers from identity theft or credit report nightmares that can follow.

"Credit card companies should enforce requirements that all online credit card databases use encryption or other methods like the SDV® to ensure they aren't compromised."

Credit card security will be one of the topics addressed at the MasterCard Asia/Pacific Future of Money Technology Fair™ and the MasterCard Asia/Pacific Market Leadership Meeting being held at the Hyatt Regency Perth from the 10 – 12 June.

MEDIA CONTACT: Donna Cole at Last Say Communications 9227 7688 or 0419 901 229m