

CYBER FEARS ON FED'S WEB PLAN

Web system opens banks to hackers

**Business
EXCLUSIVE**

By HILARY KRAMER

With little fanfare, the Federal Reserve will begin transferring the nation's money supply over an Internet-based system this month — a move critics say could open the U.S.'s banking system to cyber threats.

The Fed moves about \$1.8 trillion a day on a closed, stand-alone computer network. But soon it will switch to a system called FedLine Advantage, a Web-based technology.

Proponents say the system is more efficient and flexible. The current system is outdated, using DOS — Microsoft's predecessor to the Windows operating system.

But security experts say the threat of outside access is too big a risk.

"The Fed is now going to be vulnerable in two distinct ways. A hacker could break in to the Fed's network and have full access to the system, or a hacker might not have complete access but enough to cause a denial or disruptions of service," said George Kurtz, co-author of "Hacking Exposed" and CEO of Foundstone, an Internet security company.

"If a security breach strikes the very heart of the financial world and money stops moving around, then our financial system will literally start to collapse and chaos will ensue."

FedLine is expected to move massive amounts of money. Currently, Fedwire transfers large-dollar payments averaging \$3.5 million per transaction among



Alan Greenspan is taking the Fed high tech, but there are risks.

Federal Reserve offices, financial institutions and federal government agencies.

Patti Lorenzen, a spokeswoman for the Federal Reserve, said the agency is taking every precaution.

"Of course, we will not discuss the specifics of our security measures for obvious reasons," she said. "We feel confident that this system adheres to the highest standards of security. Without disclosing the specifics, it is important to note that our security controls include authentication, encryption, firewalls, intrusion detection and Federal Reserve conducted reviews."

Ron Gula, president of Tenable Network Security and a specialist in government cyber security, said he's sure the Fed is taking every precaution. But no system is 100 percent foolproof.

"If the motive was to manipulate the money transferring, there are Tom Clancy scenarios where there are ways to subvert underlying technologies," Gula said. "For example, a malicious programmer can put something in the Fed's network to cause the system to self-destruct or to wire them money."

The biggest concern isn't the 13-year-old who hacks into the Fedwire and sends himself some money — it's terrorism.

On July 22, the Department of

Homeland Security released an internal report saying a cyber attack could result in "widespread disruption of essential services ... damag(ing) our economy and put(ting) public safety at risk."

But the Fed's undertaking of this massive overhaul is considered a necessity.

"Our strategy is to move to Web-based technology because there are inherent limitations with DOS based technology and our goal is to provide better and robust product offerings to meet our customers' needs," said Laura Hughes, vice president of national marketing at the Chicago Fed, which has spearheaded this program.