



Reprints of articles about your community bank • www.JohnMarshallBank.com • 703.584.0840

Reston Bank Helps Tackle Cyber Fraud

The Fairfax Times

by Gregg MacDonald/reprinted from
The Fairfax Times

Reston-based John Marshall Bank is one of the fastest growing banks in the United States, according to consumer banking analysts BestCashCow.com, and that designation also makes it a prime target for cyber attacks.

"We see about 60,000 attempted online attacks or 'pings' in a typical month," said bank CEO John R. Maxwell. "Bank robbers don't always come through the front door. ... We take cybersecurity very, very seriously."

The bank today has more than 3,000 accounts and assets of about \$400 million — a 1,500 percent increase from the \$23 million it had when it opened five years ago.

The value of online thefts aimed at the financial services sector and its customers far exceeds that of physical bank robberies, according to the 2011 Norton Cybercrime Report. The report estimated the global cost of cybercrime at nearly \$400 billion per year, and said there are more than 1 million victims of cybercrime per day.

"In one of the most sophisticated and organized attacks on the financial sector, an international network of hackers recently obtained access to a financial corporation's network and completely compromised its encryption," said FBI Executive Assistant Director Shawn Henry. "They were inside the system for months doing reconnaissance,

which enabled them to steal millions of dollars in less than 24 hours when they finally took overt action.

"Another major international hacking group used an Automated Clearing House wire transfer system to access online commercial banking accounts and distribute malicious software that led financial institutions to lose nearly \$70 million."

To combat this growing threat, the FBI has formed cyber squads in each of its 56 field offices, with more than 1,000 advanced cyber-trained FBI special agents, intelligence analysts and forensic examiners, Henry said.

Trent Teyema, assistant special agent in charge of the FBI Washington Field Office's Criminal Cyber Division, recently spoke in Reston at a symposium staged by John Marshall Bank for its commercial and individual clients.

"With the threat of today's increasing Internet fraud in all aspects of society, we decided to take a proactive approach to help customers avoid financial loss by



Bruce Gemmill (left) is senior vice president and chief marketing officer for John Marshall Bank, which is based in Reston. Gemmill sits with Bill Ridenour, the bank president and chief administrative officer. John Marshall Bank recently staged a symposium on cyber crimes for its customers.

criminal schemes," said Bruce Gemmill, the bank's senior vice president.

"Our highest risk remains ACH transactions originated by our clients," said Carl Dodson, the bank's chief operating officer. "We review them daily. Before one goes through, someone here has reviewed it."

According to the FBI, actions such as this help mitigate the success of fraud attempts.

"Managing the consequences of a cyber attack entails minimizing the harm that results when an adversary does break into a system," Henry said. "An example would be encrypting data so the hacker can't read it, or having redundant systems that can readily be reconstituted in the event of an attack."

In Fairfax County, individuals also have a new weapon against financial crimes.

An online reporting system for victims of financial crimes including credit card, check and identity fraud was launched by Fairfax County police in October. It already has received in excess of 300 online reports, according to police.

"Overall, we get about 4,000 of these types of reports annually," said Fairfax County police Detective Clinton Beach, who added that the online reporting system will enhance the police department's Financial Crimes Section.

"I'm pleased to say we're having some success," Henry said. "In 2010, we arrested 202 criminals specifically for cyber intrusion — up from 159 in 2009. But we must continue to push forward, because our adversaries are relentless. They want our money, our property, and our secrets, and some seek to harm us well beyond that. Together, we can turn the tide against them and bolster the security of our nation's information, networks, and infrastructure." ★ *December 2011*