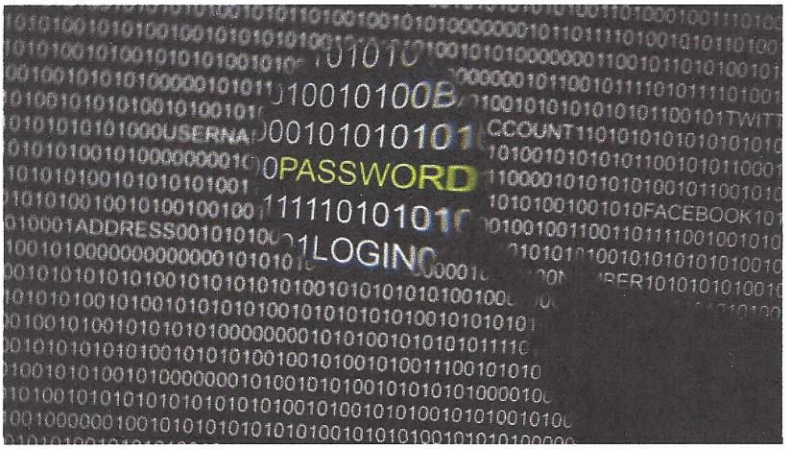
THE Fiscal TIMES
Published on *The Fiscal Times* (http://www.thefiscaltimes.com)

Is a $5 Billion Phone Hacking Scam Too Small to Nail for the FCC?



REUTERS
By Brianna Ehley,
The Fiscal Times
October 20, 2014

A broad phone hacking scheme targeting vulnerable small businesses is costing victims billions of dollars each year. Despite advocacy groups'

Increasing pressure on federal regulators to ramp up protections, very little has been done.

Digital phone hacking has been going on for years, but with the help of the Internet, hackers are more easily able to break into company phone systems and quickly bilk them out of hundreds of thousands of dollars in fraudulent phone charges. Last year, the swindle cost victims nearly $5 billion—a major jump from $1 billion in 2011, *The New York Times* reported.

According to telecommunications fraud experts, the scheme involves premium rate phone numbers—the 1-900 numbers used for psychic or sexual chat lines that charge callers more than $1 per minute.

Hackers lease these numbers then break into a business's phone system—usually a small business that doesn't have advanced security software. Using high-speed computers, they make hundreds of calls to the pay lines simultaneously- driving up the bill. The hackers then rake in a cut of the charges—up to 24 cents per minute per call.

In one instance, "hackers broke into the phone system of Foreman Seeley Fountain Architecture, a small Georgia-based architecture firm, and made $166,000 worth of calls from the firm to premium-rate telephone numbers in Gambia, Somalia and the Maldives," *The Times* noted. The complaint filed with the Federal Communications Commission said it would have taken the company 34 years to run up those charges, based on its average phone bill. Though most companies settle these charges with their phone provider, it often entails an expensive and lengthy legal process—sometimes costing thousands of dollars.

This type of fraud is so widespread that U.S. officials have even suggested that the scheme has been used to fund terrorist activities. In 2011, the FBI arrested four people for hacking into AT&T customers' servers and defrauding businesses out of more than $2 million. That money was allegedly directed to a Saudi Arabian militant group that U.S. officials say financed the 2008 Mumbai terrorist attack. AT&T eventually reimbursed all consumers.

"Premium rate numbers are begging to be used for fraud," Jim Dalton, founder of TransNexus, an Internet calling management software company, said in a statement on the company's website. "The premium rate number business model made sense before VoIP technology was available. Now, a whole eco-system has evolved that makes traffic pumping fraud to premium rate numbers an easy endeavor for anyone."

The FCC has set up guidelines about how to govern these numbers—since they are so vulnerable to fraudulent use. Consumers can submit complaints on the regulators' website. Still industry groups don't think the agency has gone far enough in protecting against these kinds of schemes.

Roberta Aronoff, the executive director of the Communications Fraud Control Association works directly with federal agencies like the FBI to help catch fraudsters. Aronoff's organization routinely flags numbers suspected of being part of the scheme—into a fraud management system so carriers can block them.

Still, lawmakers and advocates say the FCC should do more. Last year, Sen. Chuck Schumer (D-NY) called on the FCC and tech industry to increase fraud protections within cell phone companies—after a handful of small businesses in New York were slapped with fraudulent phone charges.

"Dozens of New York small businesses have fallen prey to these hackers through their voicemail systems, and are often forced to cover the cost for weeks-worth of overseas calls," Schumer said in a statement. "The telecom industry and the Federal Communications Commission must do more to detect these fraudsters, to stop or prevent the deceptive charges as quickly as possible, and to protect small business owners from the financial impact."

Since then, however, there has been little movement on any type of federal regulation or industry-wide policy aimed at dealing with these schemes. Still, it continues hampering small businesses. The FCC could not be reached for comment.

"It's relentless," TransNexus's Dalton told *The New York Times*. "People don't realize their phone is a six-figure liability waiting to happen."

Brianna Ehley
Follow on Twitter See Google Plus Page
Washington Correspondent Brianna Ehley, based in D.C., covers Congress, government agencies and spending issues, health care, and tax and economic policy for The Fiscal Times.