

**From:** Taillon, Jeff  
**To:** Godfrey, Rob <RobGodfrey@gov.sc.gov>  
Stirling, Bryan <BryanStirling@gov.sc.gov>  
Taillon, Jeff <JeffTaillon@gov.sc.gov>  
**Date:** 11/21/2012 10:26:40 AM  
**Subject:** Post and Courier: One click likely allowed hackers into breached database

---

**Post and Courier:** One click likely allowed hackers into breached database

<http://www.postandcourier.com/article/20121121/PC16/121129902/1006/one-click-likely-allowed-hackers-into-breached-database>

By Stephen Largent

COLUMBIA — With one click, hackers likely were able to have their way with an S.C. Department of Revenue database that contained millions of tax records, according to a company that investigated the breach.

In a report released Tuesday, cybersecurity firm Mandiant said it thinks that on Aug. 13, a malicious email was sent to multiple Revenue Department employees.

At least one of the employees clicked the link in the email, unknowingly executing malicious software and compromising the database, according to the company.

Mandiant wrote in its report that it was unable to determine conclusively if this is how Revenue Department employee credentials used to enter the agency's systems were obtained.

The company said it based the theory on other facts discovered during its investigation.

The release of the report Tuesday came as Gov. Nikki Haley announced the resignation of Revenue Department Director James Etter, and that only taxpayers who filed electronically were compromised in the attack. People and businesses who filed paper returns were not affected, she said.

Haley said the state will be sending notification letters to those affected. People who have signed up for credit monitoring with Experian will be notified by email.

The governor said the breach affected 3.8 million individual taxpayers, 1.9 million dependents, 699,900 businesses, 3.3 million bank accounts and 5,000 credit card accounts, all of which are now expired.

For weeks, officials had said 657,000 businesses were affected by the cyberattack. Haley explained the discrepancy Tuesday by saying the state was only 95 percent certain when it announced the earlier number.

Of Etter's resignation, Haley said she still has confidence in his abilities, but "I think Jim and I both agree that we need a new set of eyes on the Department of Revenue."

Etter will stay on the job until Dec. 31. He will be succeeded by Bill Blume, who now is serving as executive director of the new S.C. Public Employee Benefit Authority.

Haley struck a different tone Tuesday when describing Mandiant's findings and how the hackers attacked the Revenue Department. She said the state "absolutely" could have done more to prevent the breach. Previously, Haley has repeatedly said nothing could have been done to stop the attack.

The two central faults in the attack, Haley said, were that the Revenue Department didn't have dual verification to get into its system, and that Social Security numbers were unencrypted.

She said the lack of encryption was compliant with Internal Revenue Service requirements.

“Having said that, should we have done more? Yes, we should have done more than we did,” Haley said. An IRS official did not directly respond to Haley’s contention, instead offering a statement.

“Protecting taxpayer data is our top priority at the IRS,” wrote agency spokeswoman Michelle Eldridge. “We have many different systems with a variety of safeguards — including encryption — to protect taxpayer data. The IRS has in place a robust cyber security of technology, people and processes to monitor IRS systems and networks. We work closely with the states to ensure the protection of federal tax data. We have a long list of requirements for states to handle and protect federal tax information. Just as importantly, we expect the states to follow the standards of the National Institute of Standards and Technology.”

Haley said the state is in the process of encrypting all Social Security numbers on tax returns, and she released a letter she wrote to the IRS asking the agency to require all states to have stronger security measures for handling tax information.

“We have filers in South Carolina that file in other states, and they are not safe in other states as long as these numbers are not encrypted,” she said.

Eldridge said the agency has received the letter from Haley and will be reviewing it.

Officials in neighboring Georgia and North Carolina have told The Greenville News that those states’ revenue agencies encrypt all data.

Mandiant investigation

Without knowing for certain how the attackers got into the Revenue Department database, Mandiant was still able to assess other aspects of the breach.

Among the company’s findings:

The attacker compromised 44 systems. One system had malicious “backdoor” software installed. Database backups or files were stolen from three systems. The attacker accessed 39 of the 44 systems, performing activities involving passwords and reconnaissance.

The hacker used at least 33 unique pieces of malicious software and utilities to perform the attack and steal data.

The attacker used at least four valid Revenue user accounts during the attack.

Mandiant wrote that no hacker activity has been detected since the company recommended immediate changes to Revenue Department security procedures. Longer-term improvements are in the process of being put in place, according to the company.

Haley last week detailed new cybersecurity steps the state is taking. On Tuesday, she said she also will offer additional proposals for introduction in the Legislature.

Resources

**ENROLL IN FREE CREDIT MONITORING AND IDENTITY PROTECTION:** The state is paying for taxpayers to receive identity-protection services from Experian for one year. South Carolinians can enroll either online or by phone. To register by phone, call 1-866-578-5422. The hotline is open from 11 a.m. to 8 p.m. on weekends and 9 a.m. to 9 p.m. on weekdays. To register online, go to [protectmyid.com/scdor](https://protectmyid.com/scdor) and use the code “SCDOR123.” At some point, that generic code may not work, and residents will have to call the hotline number.

**PLACE A FRAUD ALERT or SECURITY FREEZE ON your credit RECORDS:** Residents can request “fraud alerts” to let potential creditors know they may be a victim of identity theft or request a “security freeze” to restrict potential creditors’ access to your credit records. To place a fraud alert, call Equifax at 1-800-685-1111, Experian at 1-888-397-3742 or TransUnion at 1-800-680-7289. To place a security freeze, you must contact each agency individually. Under South Carolina law, the consumer reporting agencies cannot charge consumers fees for placing, temporarily lifting or removing a security freeze.

**REGULARLY CHECK YOUR CREDIT REPORT:** Get free credit reports from the three largest credit-rating organizations by going to [annualcreditreport.com](http://annualcreditreport.com).

**FOR BUSINESSES:** Both Dun & Bradstreet Credibility Corp. and Experian are offering free credit-monitoring services for all South Carolina businesses that have filed state taxes since 1998. Dun & Bradstreet is offering lifetime credit-monitoring via its CreditAlert product. Visit [DandB.com/SC](http://DandB.com/SC) or call customer service toll-free at 800-279-9881. Experian is offering one year of its Business Credit Advantage product at [smartbusinessreports.com/SouthCarolina](http://smartbusinessreports.com/SouthCarolina). The deadline to sign up for the Experian service is Jan. 31. There is no deadline to sign up for the Dun & Bradstreet service.

**Who was victimized**

Gov. Nikki Haley announced Tuesday that only electronically filed tax returns were affected by the breach.

The state also now knows which returns were compromised. People affected will be notified with a letter. Those who have signed up for credit monitoring with Experian will be notified via email.

**Jeff Taillon**

(803) 734-5129|Direct Line

(803) 767-7653|Cell