State of South Carolina
Department of Revenue
300A Outlet Pointe Blvd., Columbia, South Carolina 29210
P.O. Box 125, Columbia, South Carolina 29214

C-450 (Rev. 8/29/12) 6371

For Immediate Release:

October 26, 2012

Contact: Rob Godfrey
Office of Gov. Nikki Haley
(803) 734-5074 (803) 429-5086

Samantha Cheek
SC Department of Revenue
(803) 898-5281

SC Department of Revenue Responds to Cyber Attack, Will Provide Credit Monitoring and Identity Theft Protection to Taxpayers

Hacker illegally obtained credit card and Social Security numbers

[Columbia, S.C.] The S.C. Department of Revenue today announced that approximately 3.6 million Social Security numbers and 387,000 credit and debit card numbers have been exposed in a cyber attack. Of the credit cards, the vast majority are protected by strong encryption deemed sufficient under the demanding credit card industry standards to protect the data and cardholders. Approximately 16,000 are unencrypted.

To protect taxpayers, the state will provide those affected with one year of credit monitoring and identity theft protection. Officials emphasized that no public funds were accessed or put at risk.

“On October 10, the S.C. Division of Information Technology informed the S.C. Department of Revenue of a potential cyber attack involving the personal information of taxpayers,” said DOR Director James Etter. “We worked with them throughout that day to determine what may have happened and what steps to take to address the situation. We also immediately began consultations with state and federal law enforcement agencies and briefed the governor’s office.”

Upon the recommendation of law enforcement officials, DOR contracted Mandiant, one of the world’s top information security companies, to assist in the investigation, help secure the system, install new equipment and software and institute tighter controls on access.

On October 16, investigators uncovered two attempts to probe the system in early September, and later learned that a previous attempt was made in late August. In mid-September, two other intrusions occurred, and to the best of the department’s knowledge, the hacker obtained data for the first time. No other intrusions have been uncovered at this time. On October 20, the vulnerability in the system was closed and, to the best of the department’s knowledge, secured.

“The number of records breached requires an unprecedented, large-scale response by the Department of Revenue, the State of South Carolina and all our citizens,” said Governor Nikki Haley. “We are taking immediate steps to protect the taxpayers of South Carolina, including providing one year of credit monitoring and identity protection to those affected.”

Anyone who has filed a South Carolina tax return since 1998 is urged to visit protectmyid.com/scdor or call 1- 866-578-5422 to determine if their information is affected. If so, the taxpayer can immediately enroll in one year of identity protection service provided by Experian.

Experian's ProtectMyID™ Alert is designed to detect, protect and resolve potential identity theft, and includes daily monitoring of all three credit bureaus. The alerts and daily monitoring services are provided for one year, and consumers will continue to have access to fraud resolution agents and services beyond the first year.

In addition to the Experian service, state officials urged individuals to consider additional steps to protect their identity and financial information, including:

- Regularly review credit reports;
- Place fraud alerts with the three credit bureaus;
- Place a security freeze on financial and credit information with the three credit bureaus.

If credit card information is compromised, the best protection is to have the bank reissue the card. Anyone who has used a credit card in a transaction with the Department of Revenue should check bank accounts regularly to see if any unauthorized charges have occurred. If so, the cardholder should contact the credit card issuer immediately by calling the toll-free number located on the back of the card or on a monthly statement, tell them what you have seen, and ask them to cancel and reissue the card. Consumers should also change any credit card web account passwords immediately when unauthorized charges are detected.

"From the first moment we learned of this, our top priority has been to protect the taxpayers and the citizens of South Carolina, and every action we've taken has been consistent with that priority," Etter said. "We have an obligation to protect the personal information entrusted to us, and we are redoubling our efforts to meet that obligation."

###

Chronology

October 10:

- The SC Department of Revenue was informed by the South Carolina Division of Information Technology (DSIT) of a potential cyber attack involving the personal information of taxpayers.
- DOR worked with DSIT throughout the day to determine what may have happened and what steps needed to be taken immediately to deal with the situation.
- DOR consulted with state and federal law enforcement agencies for guidance.
- Law enforcement recommended several steps to be taken, including consulting the nation's top cyber security firms.
- DOR assessed the top 3 recommendations from law enforcement and contacted Mandiant of Alexandria, VA.
- DOR contacted the Governor's office.
- SLED Chief Keel briefed Governor Haley.

October 11:

- DOR met with the Governor's office in the morning to give her a full briefing, including laying out our 4-pronged approach:
    - Contract with Mandiant, which we signed on October 12 with the approval of the Governor, to find and fix the leak;
    - Conduct an internal investigation of all outside contractors and certain employees to see if they have been involved with any security breaches;
    - Develop of a public notification plan;
    - Institute additional protection tools on our system.
- DSIT began monitoring DOR and its main servers to detect any unauthorized intrusions.
- DOR made the decision that if DSIT or DOR identified any unusual exfiltrations of data, the system impacted would be shut down immediately.

October 12:

- DOR signed a contract with Mandiant.
- Mandiant began working on plans to send surveillance and monitoring tools to be installed at DOR in SC.

October 15:

- DOR worked with Mandiant to begin installing surveillance and monitoring equipment which was completely in place within 48 hours.
- DOR began daily status update calls with complete team, including representatives from law enforcement, DSIT, DOR, Mandiant- the first call was planning session.

October 16:

- Mandiant began deploying a monitoring agent on every computer workstation throughout DOR, a process was completed by October 20.

- By the daily status call on Oct. 16, Mandiant was able to confirm that an unknown hacker or hackers probed the system in early September. We also learned that in mid-September, two other intrusions occurred, and to the best of our knowledge, the hacker obtained data for the first time.

October 18:

- Daily team status meetings were held and systems were continuously monitored.

October 19:

- Mandiant sent a four member team to begin the on-site investigation at DOR.
- DOR is still managing day-to-day business of state of SC while managing this major issue.
- DOR contacted South Carolina law firm, Nelson Mullins, about getting assistance with breach management.

October 20:

- The "hole" was closed and system was secured, to the best of our current knowledge.

October 21-25:

- We continued to monitor the system to make sure no more data was compromised.
- The number of records breached requires an unprecedented, large-scale response by the Department of Revenue, the State of South Carolina and all our citizens.
- We confirmed that <u>NO public funds</u> were accessed or put at risk as those servers are completely separate from those that were breached.
- However, approximately 3.6 million Social Security numbers may be affected. Approximately 387,000 credit card numbers were in the materials that were taken, but approximately 371,000 are protected by strong encryption deemed sufficient under the demanding credit card industry standards to protect the data and cardholders, and the others are dated from before 2003.

<u>Safety Precautions:</u>

- We are taking immediate steps to protect the taxpayers of South Carolina, including providing one year of credit monitoring to those who may be affected through Experian's ProtectMyID Alert. This service includes:
    - A free credit report;
    - Daily credit monitoring across three credit bureaus to detect any suspicious activity;
    - A $1 million identity theft insurance policy.
- <u>The public is urged to be aware of scams. DOR will never call or otherwise contact those affected asking for personal information. Beneficiaries are advised to never give out their Social Security numbers or other identifying information to people you do not know.</u>
- If you filed a South Carolina tax return since 1998, you are urged to call the toll-free call center that DOR has established, which will be operating 24/7 beginning at noon on Friday, October 26, 2012,for anyone who wishes to know if their personal information was included and to immediately enroll in one year of credit monitoring: 1-866-578-5422. Also please visit: ProtectMyID.com/SCDOR.
- Please see list of additional Consumer Safety Solutions.

Consumer Safety Solutions

You can help prevent your information from being misused by taking some of the following simple steps.

In addition to these steps, the South Carolina Department of Revenue will be protecting the taxpayers of South Carolina, by providing one year of credit monitoring to those who may be affected through Experian's ProtectMyID Alert. This service includes:

- A free credit report;
- Daily credit monitoring to detect suspicious activity;
- A $1 million identity theft insurance policy.

The public is urged to be aware of scams. DOR will never call or otherwise contact those affected asking for personal information. Beneficiaries are advised to never give out their Social Security numbers or other identifying information to people you do not know.

If you filed a South Carolina tax return since 1998, you are urged to call the toll-free call center that DOR has established, which will be operating 24/7 beginning noon on Friday, October 26, 2012, for anyone who wishes to know if their personal information was included and to immediately enroll in one year of credit monitoring: 1-866-578-5422. Also please visit ProtectMyID.com/scdor for more information.

1. Review Your Credit Reports and Bank Statements. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. You can receive free credit reports by placing fraud alerts and through your credit monitoring. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement.

2. **Contact Credit/Debit Card Issuer.** When credit/debit card information is compromised, the best protection is reissue of the card. So to protect yourself from the possibility of unauthorized charges, we recommend that you check your bank account statements regularly. If you detect any

unauthorized charges, we strongly suggest that ***you contact your credit/debit card issuer immediately by calling the toll-free number located on the back of your card or on your monthly statement, tell them what you have seen, and ask them to cancel and reissue the card.*** You should tell your credit/debit card issuer that your account may have been compromised and review all charges on your account for potentially fraudulent activity. We also recommend that you change your credit/debit card web account password immediately when you discover unauthorized charges.

3. Place Fraud Alerts with the three credit bureaus. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-800-525-6285
P.O. Box 740241
Atlanta, GA 30374-0241
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9532
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
Fraud Victim Assistance Division
P.O. Box 6790
Fullerton, CA 92834-6790
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review.

4. Security Freeze: By placing a freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above in writing to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. In South Carolina, there is no charge to you for placing, thawing or lifting the freeze.

Credit Bureaus

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
www.freeze.equifax.com

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze

TransUnion Fraud Reporting
1-800-680-7289
Fraud Victim Assistance Division
P.O. Box 6790
Fullerton, CA 92834-6790
http://freeze.transunion.com

5. You Can Obtain Additional Information about the steps you can take to avoid identity theft from the following:

For South Carolina Residents:
South Carolina Office of the Attorney General
The Honorable Alan Wilson
P.O. Box 11549
Columbia, S.C. 29211
1-803-734-3970
www.scag.gov

South Carolina Department of Consumer Affairs:
1-800-922-1594 (Toll-Free)
803-734-4200
scdca@scconsumer.gov
Mailing Address:
PO Box 5757
Columbia SC 29250-5246
www.consumer.sc.gov

For all U.S. Residents:
Identity Theft Clearinghouse
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.consumer.gov/idtheft
1-877-IDTHEFT (438-4338)
TDD: 1-202-326-2502