ABOUT THE SOUTH CAROLINA DEPARTMENT OF REVENUE CYBER-ATTACK

Please note: the details of this crime and the authorities' responses have not been fully revealed. South Carolina may take more steps than those listed in this memo to help protect victims. We have prepared this memo based on the events that have been confirmed by the Governor as of October 30, 2012 to help address your initial concerns.

THE ISSUE

On October 26, 2012, the South Carolina Department of Revenue (SCDOR) announced that approximately 3.6 million Social Security numbers and 387,000 credit and debit card numbers were exposed in an unprecedented cyber-attack. Governor Nikki Haley later announced that 657,000 businesses are also at risk. Those affected include anyone who has filed a South Carolina income tax return since 1998 and those who have transacted with the SCDOR using credit or debit cards.

SHOULD YOU BE CONCERNED?

Yes. The dangers from this attack are real and could affect you as follows:

1) Thieves can use your stolen credit and debit card information to make purchases. Thanks to strict credit card industry standards, the majority of current credit cards were (and are) protected with strong encryption. However, these standards do not apply to credit cards issued before 2003 and approximately 16,000 of the credit and debit card numbers stolen were from those issued before 2003. Although credit card companies may be lenient, banks are more likely to hold you liable for unauthorized charges.

2) An identity thief could file a false tax return in your name. The taxing authorities have no ability to confirm that the taxpayer named on the return was the person who filed the return. A thief could prepare a tax return using information similar to prior year returns (but a different address) and claim a refund of taxes he or she obviously did not pay. Generally, the taxing authorities will not hold you responsible for a fraudulent filing; however, the process of correcting the issue can be frustrating and time-consuming.

3) A thief could file for credit, become employed, or receive medical services in your name. He could also sell your information to other thieves.

4) A thief could use the information to persuade you into making yourself vulnerable. By demonstrating that he has personal knowledge about your life, a thief might be able to make you feel comfortable in giving up sensitive information. Moreover, thieves intentionally use personal information for impersonation phishing scams - by posing as your banker or investment adviser, thieves may convince you to give them your online or phone password, account numbers, etc.

WHAT CAN YOU DO?

While you can't entirely control whether you will become a victim of identity theft, you can take some steps to minimize your risk:

1) **Sign Up for Credit Monitoring**
   To help alleviate the impact of the breach for *individuals*, the South Carolina government has arranged for limited protection to be available to the victims. If you have filed a South Carolina return since 1998 or have used a credit or debit card to transact with the SCDOR, you are eligible for one year of credit monitoring through Experian's ProtectMyID Alert. You can call 1-866-578-5422 to speak with an agent for over-the-telephone enrollment of this service. Or, if you prefer to sign up online you can visit www.protectmyid.com/scdor and use the activation code: scdor123

   Whether you sign up by phone or online, you will be required to answer a series of questions about your history (such as a former street address). Understandably, you may be concerned about the personal nature of these questions; we share this concern, but these questions are necessary to confirm that you are who you purport to be.

   By signing up for credit monitoring, you can receive:

   - A free copy of your Experian credit report.
   - Daily monitoring by the three major credit bureaus which alerts you of suspicious activity including new inquiries, newly opened accounts, delinquencies, or medical collections found on your Experian, Equifax, and TransUnion credit reports.
   - Identity theft resolution: If you have been a victim of identity theft, you will be assigned an Experian Identity Theft Resolution Agent who will walk you through the fraud resolution process.
   - ExtendCARE: Full access to the same personalized assistance from a Fraud Resolution Agent even after your initial ProtectMyID membership expires.
   - $1 Million Identity Theft Insurance: As a ProtectMyID member, you will be covered by a $1 million insurance policy that can help you cover certain costs including lost wages, private investigator fees, and unauthorized electronic fund transfers.

   To help alleviate the impact of the breach for *businesses*, the South Carolina government has announced that affected businesses will be given free access to Dun & Bradstreet Credibility Corp's CreditAlert. This alerts customers to changes in their business credit files. The service will be available to businesses at no charge for the life of the business. To sign up, please call 1-800-279-9881 or visit www.dandb.com/SC.

Senator Lindsey Graham is working with the IRS in an attempt to allow a business to change its federal employer identification number; however, as of the date of this memo this issue has not been resolved.

2) **Monitor Your Credit Card Statements and Bank Statements**
   If you have used your credit or debit card to transact with the SCDOR, you should monitor your monthly statements for unauthorized charges.

   The best remedy for stolen credit or debit card information is card reissuance. If you discover that your credit or debit card information has been compromised, immediately contact your credit or debit card issuer by calling the toll-free number on the back of your card or on your monthly statement. When you speak with the issuer, describe to them the unauthorized charges, request the particular card be cancelled, and request the issuance of a new card. We also recommend that you change your credit or debit card web-account password immediately to prevent future exploits.

   Fortunately, Governor Haley has disclosed that the majority of the exposed card numbers were expired credit and debit cards.

3) **Use Fraud Alerts**
   You should consider placing a fraud alert with one of the three major credit bureaus by phone and by visiting Experian's website. The credit bureaus share this information with one another. Once a credit bureau confirms the alert, the other two bureaus are automatically notified to place alerts on their records so you do not need to contact all three. A fraud alert tells creditors to follow certain procedures, such as calling 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.

4) **Place a Security Freeze**
   This step goes beyond the use of fraud alerts. By placing a freeze, you are preventing creditors from checking your credit history, thereby eliminating the chance that someone could use your identity to establish credit. You will need to contact all three national credit-reporting bureaus (contact information listed below) in writing. Please keep in mind that after 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 a freeze.

While South Carolina is paying for one year of credit monitoring, we recommend that you sign up for this service indefinitely. By using this service and remaining vigilant, you will greatly decrease your risk.

Contact one of the following to place a fraud alert:

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

Write to all three of the following to place a security freeze:

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
Fraud Victim Assistance Division
P.O. Box 6790
Fullerton, CA 92834-6790
http://freeze.transunion.com

You can get additional information on avoiding identity theft by contacting the following:

For South Carolina Residents:

South Carolina Department of Consumer Affairs
1-800-922-1594 (Toll-Free)
P.O. Box 5757
Columbia, SC 29250-5246
scdca@scconsumer.gov
www.consumer.sc.gov

For all U.S. Residents:

Identity Theft Clearinghouse Federal Trade Commission
1-877-IDTHEFT (438-4338)
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.consumer.gov/idtheft