State of South Carolina
Department of Revenue

S1 P1 **AUTO3-DIGIT 296 PLT1
Sam A. Sample
321 Any Street
Anytown, AS 12345-6789

Re: Data Breach Notification

Dear SC Taxpayer,

Tax returns and other data at the South Carolina Department of Revenue were exposed due to a security breach that took place in September 2012 and was discovered in October 2012. The information exposed in this breach included any South Carolina state taxes filed electronically by businesses or individuals since 1998, and could include social security numbers, tax identification numbers, and payment information including bank accounts and credit cards. We are writing you as an electronic filer of state taxes during the exposure period to notify you that your tax information may have been exposed in this incident.

South Carolina immediately involved state and federal law enforcement agencies to assist us in determining how to proceed, and has acted upon their advice. The Department also hired outside forensic and other experts to protect the data on its networked systems. The Department continues to monitor this situation carefully and has increased its internal review procedures to watch for any unusual activity. The breach was stopped and new technology and policy protections have been introduced to the Department to prevent further information exposure.

While the Department of Revenue has not seen evidence that any of the exposed data was used for identity theft or other crime, we took immediate steps to protect the taxpayers of South Carolina, including providing one year of credit monitoring and fraud resolution services through Experian®'s ProtectMyID® Alert program to those who may be affected. This service includes identity theft resolution services that do not expire, a free credit report, daily credit monitoring across three credit bureaus to detect any suspicious activity, and an identity theft insurance policy, including coverage of electronic fund transfers from your bank account, worth up to a million dollars*. The Department of Revenue is also providing protection for your minor dependents under Experian's Family Secure® program.

You can register for these services by visiting www.protectmyid.com/scdor, and entering the following enrollment code: **SCDOR123**. If you do not have an Internet connection, call 1-866-578-5422 to begin the enrollment process.

For tips for avoiding identity theft, you may visit www.consumer.sc.gov and click the "Identity Theft Resources" button. **We urge you to be aware of scams.** The state of South Carolina *will never call or otherwise contact those affected to ask for personal information*. Never give out your social security number or other identifying information to people you do not know or who contact you.

*Identity Theft Insurance underwritten by insurance company subsidiaries or affiliates of Chartis Inc. Please refer to the actual policies for complete terms, conditions, and exclusions of coverage.

In addition to protection from www.protectmyid.com/scdor, here are other ways to protect your families:

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:

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 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. The laws of your state govern and may limit the cost of a freeze. In any event, the cost of placing, lifting or removing the freeze is no more than $10 for each credit bureau. Contact information is as follows:

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 Maryland Residents:

Office of the Attorney General of Maryland
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
www.oag.state.md.us/Consumer
Telephone: 1-888-743-0023

For North Carolina Residents:

Office of the Attorney General of North Carolina
9001 Mail Service Center
Raleigh, NC 27699-9001
www.ncdoj.com/
Telephone: 1-919-716-6400

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