ECKERT SEAMANS
ATTORNEYS AT LAW

Eckert Seamans Cherin & Mellott, LLC
U.S. Steel Tower
600 Grant Street, 44th Floor
Pittsburgh, PA 15219

TEL 412 566 6000
FAX 412 566 6099
www.eckertseamans.com

Sandy B. Garfinkel
412.566.6868
sgarfinkel@eckertseamans.com

June 2, 2016

VIA U.S. MAIL

Office of the New Hampshire
Attorney General
33 Capitol Street
Concord, NH 03301

Re: *Data Security Incident Involving Personal Information*

To Whom It May Concern:

My firm represents SD Associates P.C. ("SD"), a firm that provides certified public accounting services to individuals and companies. I write to you concerning an incident involving cyber intrusion and theft of personal information from SD's computer system.

The incident occurred during the period of April 21-27, 2016. The stolen information included names, addresses and social security numbers of clients of SD. It was used in a limited number of cases to file false electronic tax returns with the IRS in order to obtain refunds in the names of certain SD's clients. SD has already provided written notification of the incident to those particular individuals, none of whom were New Hampshire residents.

SD learned of the incident when it was contacted by the IRS on April 27, 2016 and SD promptly commenced an investigation, including retaining a forensic computer consultant to perform an analysis of the incident. On May 19, 2016, the consultant provided a report to SD which contained the conclusion that more information had been exposed than was originally believed. Information concerning approximately 7,000 individuals was potentially compromised as a result of the incident, including, to the best of SD's knowledge at this point, 4 New Hampshire residents.

SD's technology consultants determined the manner in which the hack occurred and have upgraded SD's system security. SD is in the process of providing formal written notification to all affected individuals. A copy of the form of notice to be sent to the affected New Hampshire residents is attached hereto. The notices will be sent on approximately June 7, 2016 via U.S. Mail. SD is also providing, at its sole cost, the option for each affected person to enroll in a

ECKERT SEAMANS
ATTORNEYS AT LAW

credit and identity theft protection program for one (1) year, furnished through a nationally recognized identity theft vendor.

If you have any further questions about the incident, do not hesitate to contact me.

Very truly yours,

Sandy B. Garfinkel

Enclosures

SD Associates P.C.
Certified Public Accountants & Business Advisors

May ___, 2016

Mr. and Mrs. John Q. and Jill R. Smith
123 Anystreet
Anytown, PA 00000

Data Security Incident Involving Personal Information

Dear Mr. and Mrs. Smith:

We are writing to inform you that on April 26, 2016, SD Associates was informed by the IRS Criminal Division that data within our database concerning some of our clients was compromised. Some of that data was used to file phony electronic tax returns by criminals who sought to obtain refunds from the IRS using the stolen information. Since receiving this alarming news, we have hired a forensic computer consultant to examine our systems and to determine the extent of the unauthorized access. This past Thursday May 19, 2016, our consultants gave us a report of their conclusions.

Although the criminals do not appear to have used any of your data to file a false return, our experts have determined that your data may have been exposed or stolen during the cyber attack. Because it is possible that your information was viewed or taken by unauthorized individuals, it is also possible that your information could be misused at some later date.

We have learned from the State of Pennsylvania Bureau of Professional Affairs, that cyber criminals have engaged in similar attacks against accounting firms across the State.

The breach of our security involved the possible unauthorized disclosure of your name, social security number and address.

Please be assured that we are taking every step necessary to address this incident and that we are committed to fully protecting all of the information that you have entrusted to us. Our computer consultants have upgraded our security to prevent any further unlawful entry.
We have also notified the three major U.S. credit reporting agencies of this incident and have given those agencies a general report alerting them to the facts. To protect you, we have retained Experian, a specialist in identity theft protection, to provide you with a one year membership in Experian's ProtectMyID Alert identity theft detection services, free of charge. You can enroll in the program by following the directions below.

Please keep this letter; you will need the personal access code it contains in order to register.

Activate ProtectMyID Now in Three Easy Steps

1. Ensure that you enroll by _____ __, 2016 (Your code will not work after this date.)
2. Visit the ProtectMyId Web Site to enroll: www.protectmyid.com/redeem
3. Provide Your Activation Code: **<Code>**

SD Associates P.C.
Certified Public Accountants & Business Advisors

If you have questions or need an alternative to enrolling online, please call 877-371-7902 and provide engagement # **<Number>**

We urge you to take precautionary action now to help prevent and detect any misuse of your information.

In order to minimize future occurrence of the identity theft fraudulent filing we recommend you apply for the IRS Identity Protection Pin , the link is provided below. This will prevent any tax return from being filed electronically unless the pin is present, this pin must also be provided to SD Associates so we can complete any future individual tax returns on your behalf. The system is currently being revised and will be activated shortly.

https://www.irs.gov/individuals/get-an-identity-protection-pin
Telephone number : 1-800-908-4490, Monday - Friday, 7 a.m. - 7 p.m.

You are urged to be vigilant for signs of fraud or identity theft by reviewing your account statements regularly and obtaining and reviewing your free credit report concerning your credit activity. There are instructions for obtaining your free credit report in the attached pages. If you suspect that fraud or identity theft has occurred, you should report it to your local law enforcement agency, to your state's attorney general's office and/or to the U.S. Federal Trade Commission ("FTC") (contact information for the FTC is provided in the attached pages).

Even if you do not find any suspicious activity on your initial credit reports, the FTC recommends that you check your credit reports periodically. Checking your credit reports periodically can help you spot problems and address them quickly.

We are grateful for your affiliation and take your confidence and the confidential nature of our relationship very seriously. We believe we have taken all necessary precautions to prevent further compromise of your personal information and we are taking every step to avoid harm to you and your credit. We sincerely apologize for this incident, regret any inconvenience it may cause you and hope that, by acting responsibly and promptly, we will avert any further harm.

Of course, we welcome your call to further discuss this matter. We are available to answer any questions you may have. Please contact Howard Siegal 215-517-5600 .

Thank you.
Sincerely,
SD Associates, PC

SD Associates P.C.
Certified Public Accountants & Business Advisors

ADDITIONAL RESOURCES, CREDIT ALERTS AND FREEZES

Information about Identity Theft

Federal Trade Commission
The Federal Trade Commission provides helpful information about how to avoid identity theft.

- Visit: http://www.ftc.gov/idtheft
- Call (toll-free): 1-877-ID-THEFT (1-877-438-4338)
- Write: Consumer Response Center, Federal Trade Commission, 600 Pennsylvania Ave., NW, Washington, DC 20580
- It is recommended that you report suspected identity theft to law enforcement, including the Federal Trade Commission

Free Annual Credit Reports

You may obtain a free copy of your credit report once every 12 months.

- Visit: http://www.annualcreditreport.com
- Call (toll-free): 1-877-322-8228
- Write: Complete an Annual Credit Report Request Form and mail it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281 (you can print a copy of the form at http://www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf).

You also may purchase a copy of your credit report by contacting one of the three national credit reporting companies.

Equifax 1-800-525-6285 www.equifax.com P. O. Box 740241 Atlanta, GA 30374-0241	Experian 1-888-397-3742 www.experian.com P. O. Box 9554 Allen, TX 75013	TransUnion 1-800-888-4213 www.transunion.com 2 Baldwin Place P.O. Box 1000 Chester, PA 19022

Fraud Alerts: "Initial Alert" and "Extended Alert"

You can place two types of fraud alerts on your credit report to put your creditors on notice that you may be a victim of fraud: an "Initial Alert" and an "Extended Alert." An Initial Alert stays on your credit report for 90 days. You may ask that an Initial Alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An Extended Alert stays on your credit report for seven years. To obtain the Extended Alert, you must provide proof to the credit reporting company (usually in the form of a police report) that you actually have been a victim of identity theft. You have the right to obtain a police report regarding the data security incident. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three credit reporting companies provided above.

A potential drawback to activating a fraud alert would occur when you attempt to open a new account. You would need to be available at either your work phone number or home phone number in order to approve opening the new credit account. If you are not available at either of those numbers, the creditor may not open the account. In addition, it may take longer to obtain credit and in some cases merchants may be hesitant to open a new account.

Fraud alerts will not necessarily prevent someone else from opening an account in your name. A creditor is not required by law to contact you if you have a fraud alert in place. Fraud alerts can legally be ignored by creditors. If you suspect that you are or have already been a victim of identity theft, fraud alerts are only a small part of protecting your credit. You also need to pay close attention to your credit report to make sure that the only credit inquiries or new credit accounts in your file are yours.

You may contact all of the three major credit reporting agencies using the information below that they have published. Credit agencies will need to verify your identity which will require providing your Social Security number and other similar information.

TransUnion
P.O. Box 2000
Chester, PA 19022-2000
https://fraud.transunion.com
1-800-680-7289

Equifax
P. O. Box 740241
Atlanta, GA 30374-0241
https://www.alerts.equifax.com/AutoFraud_Online/jsp/fraudAlert.jsp
1-888-766-0008

Experian
P. O. Box 9554
Allen, TX 75013
https://www.experian.com/fraud/center.html
1-888-397-3742

Placing a fraud alert does not damage your credit or credit score. Additional information may be obtained from www.annualcreditreport.com.

Credit or Security Freeze on Credit File

Consumers may also place a security freeze on their credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, mortgages, employment, housing or other services.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent; however, using a security freeze may interfere with or delay your ability to obtain credit. To place a security freeze on your credit report, contact the credit reporting agencies using the information below, and be prepared to provide the following (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well):

(1) Full name, with middle initial and any suffixes;
(2) Social Security number;
(3) date of birth;
(4) Current address and any previous addresses for the past two years; and
(5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles.

The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. In Massachusetts, consumer reporting agency may charge a fee of no more than $5.00 to place, lift, and/or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and you have submitted a valid police report relating to the identity theft incident to the consumer reporting agency. The addresses of consumer reporting agencies to which requests for a security freeze may be sent are:

TransUnion
P.O. Box 2000
Chester, PA 19022-2000
https://freeze.transunion.com

Equifax
Equifax Security Freeze
P.O. Box 105788
Atlanta, Georgia 30348
https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp

Experian
P. O. Box 9532
Allen, TX 75013
https://www.experian.com/freeze/center.html

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include:

- proper identification (name, address, and Social Security number);
- the PIN or password provided to you when you placed the security freeze; and

- the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available.

The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.