

August 30, 2016

Mr. Bob Ferguson
Attorney General
Washington State Office of the Attorney General
1125 Washington Street SE
P.O. Box 40100
Olympia, WA 98504

Re: Security Incident Notice

Dear Attorney General Ferguson:

I represent Presnell Gage, PLLC, headquartered in Lewiston, Idaho. This letter is being sent pursuant to Wash. Rev. Code §§ 19.255.010-.020 because Presnell Gage determined on August 18, 2016 that 2,613 residents of Washington may have had their names, Social Security numbers and bank account numbers affected by an information security incident.

Presnell Gage recently learned that a number of its clients had tax returns filed in their names without their authorization. It immediately investigated whether its information system had been accessed without authorization. On August 18, 2016 it determined that client files may have been accessed without authorization between July 16, 2016 and August 18, 2016.

Presnell Gage notified the Internal Revenue e-File Services Department, the Internal Revenue Service/Criminal Investigation and the Federal Bureau of Investigation about the incident, and will provide whatever cooperation is necessary to protect client tax information and hold the perpetrator(s) accountable. The security of its system has been enhanced, making it more difficult for similar incidents to occur in the future.

Presnell Gage is in the process of notifying all affected consumers with the attached letter. As referenced in the letter, they will provide 36 months of credit monitoring and identity protection services to affected consumers through AllClear ID.

Please contact me should you have any questions.

Sincerely,

Davis Wright Tremaine LLP



Sean B. Hoar

cc: Philip J. Nuxoll, Managing Member
Presnell Gage, PLLC



August 31, 2016

Subject: Data Security Incident

I am writing to inform you of a data security incident that has affected your personal information. We take the privacy and security of your information very seriously. This is why I am contacting you, offering you credit monitoring and identity protection services, and informing you about steps that can be taken to protect your personal information.

What happened? We recently learned that a number of our clients had tax returns filed in their names without their authorization. We immediately investigated whether our information system had been accessed without authorization. On August 18, 2016, we determined that client files may have been accessed without our authorization between July 16, 2016 and August 18, 2016. It appears that your tax return file was one of the files accessed.

What Information Was Involved? The information included names, addresses, dates of birth, Social Security numbers and bank account numbers if electronic deposit or payment options were used with tax returns.

What Are We Doing? We are notifying you of the incident, providing you information about steps you can take to protect your personal information, and offering you credit monitoring and identity protection services for 36 months at no cost to you. We also notified the Internal Revenue e-File Services Department, the Internal Revenue Service/Criminal Investigation and the Federal Bureau of Investigation, and will provide whatever cooperation is necessary to protect your tax information and hold the perpetrator(s) accountable. The security of our system has been enhanced, making it more difficult for similar incidents to occur in the future.

What You Can Do: We have arranged to have AllClear ID protect your identity for 36 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 36 months.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 877-676-0379 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Credit Monitoring: This service offers additional layers of protection including credit monitoring and a \$1 million identity theft insurance policy. To use this service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by telephone by calling 877-676-0379 using the following redemption code: «Redemption_Code». For a child under 18 years old, AllClear ID ChildScan identifies acts of credit, criminal, medical or employment fraud against children by searching thousands of public databases for use of your child's information. Please note that additional steps may be required by you in order to activate your telephone alerts and monitoring options.

We will also complete, on your behalf, IRS Form 14039, an Identity Theft Affidavit, which we will submit to the IRS. You can view this form at <http://www.irs.gov/pub/irs-pdf/f14039.pdf>. Please contact us should you have any questions about it. If you have other identity theft/tax related issues, contact the IRS Identity Protection Specialized Unit at 1-800-908-4490.

For More Information: Further information about how to protect your personal information appears on the following pages. Should you have any questions, please contact AllClear ID at 877-676-0379 or support@allclearid.com. You may also contact the person in charge of your account or one of us listed below. Please accept our sincere apologies and know that we deeply regret any worry or inconvenience this may cause you.

Philip J. Nuxoll, CPA
Managing Member
(208) 746-8281
philnuxoll@presnellgage.com

Mitch Marx, CPA
Management Group Member
(208) 746-8281
mmarx@presnellgage.com

Jackson Davis, CPA
Management Group Member
(208) 882-2211
jdavis@presnellgage.com

Sandy R. Wallace, CPA
Director of Operations/HR
(208) 746-8281
swallace@presnellgage.com

www.presnellgage.com

Sincerely,



Philip J. Nuxoll, CPA
Managing Member

Information About Protecting Personal Information

Review Your Account Statements and Notify Issuing Bank & Law Enforcement of Suspicious Activity:

It is recommended that you remain vigilant for any incidents of fraud or identity theft by regularly reviewing credit card account statements and your credit report for unauthorized activity. If you detect any suspicious activity on an account, we recommend you contact your issuing bank immediately to either freeze or close the account. You may also report any fraudulent activity or any suspected identity theft to local law enforcement, the Federal Trade Commission (FTC), or your respective state Attorney General. Residents of Massachusetts and Rhode Island have the right to obtain any police report filed in regard to this incident.

Copy of Free Credit Report: You may obtain a free copy of your credit report from the following national consumer reporting agencies or from the Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281, 1-877-322-8228, www.annualcreditreport.com:

Equifax: P.O. Box 740241, Atlanta, Georgia 30374-0241, 1-800-685-1111, www.equifax.com

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

TransUnion: P.O. Box 1000, Chester, PA 190222, 1-800-888-4213, www.transunion.com

Additional Free Resources on Identity Theft: You can obtain information from the consumer reporting agencies, the **FTC**, or your respective state Attorney General about steps you can take toward preventing identity theft. The FTC may be contacted at **FTC, Consumer Response Center**, 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-438-4338, www.ftc.gov/idtheft.

For residents of Maryland, North Carolina, and Rhode Island: Residents of Maryland, North Carolina and Rhode Island can also obtain information about preventing and avoiding identity theft from their attorneys general at the addresses below, and from the Federal Trade Commission.

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

North Carolina Office of the
Attorney General
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226
www.ncdoj.com

Rhode Island Office of the
Attorney General
150 South Main Street
Providence, RI 02903
(401) 274-4400
<http://www.riag.ri.gov>

Fraud Alerts: There are two types of fraud alerts that you can place 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. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national consumer reporting agencies listed below:

Equifax: 1-888-766-0008, www.equifax.com

Experian: 1-888-397-3742, www.experian.com

TransUnion: 1-800-680-7289, fraud.transunion.com

Credit Freezes (for Non-Massachusetts Residents): You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally \$5 to \$20 per action at each credit reporting agency. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major consumer reporting agencies as specified below to find out more information:

Equifax: P.O. Box 105788, Atlanta, GA 30348, www.equifax.com

Experian: P.O. Box 9554, Allen, TX 75013, www.experian.com

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

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national consumer reporting agencies listed above.