MULLEN COUGHLIN LLC

STATE OF NH
DEPT OF JUSTICE
2017 FEB 27 PM 12: 03

Edward J. Finn
Office: 267-930-4776
Fax: 267-930-4771
Email: efinn@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

February 22, 2017

VIA U.S. MAIL
Attorney General Joseph Foster
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Attorney General Foster:

We represent InterMountain Management, LLC ("InterMountain"), 2390 Tower Drive, Monroe, Louisiana 71201, and are writing to notify your office of an incident that may affect the security of personal information relating to approximately one (1) New Hampshire resident. The investigation into this event is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, InterMountain does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Nature of the Data Event

InterMountain was the victim of an email spoofing attack on February 3, 2017, by an individual pretending to be InterMountain's owner. A request was made for all 2016 W-2 forms prepared by InterMountain. Unfortunately, copies of all 2016 W-2 forms prepared by InterMountain (both for its direct employees and for individuals employed by InterMountain's client businesses to whom InterMountain provides management services) were provided before it was discovered that the request was made from a fraudulent account. InterMountain discovered the fraudulent nature of the request on February 6, 2017, and has been working tirelessly to investigate and to mitigate the impact of the attack.

Notice to New Hampshire Resident

Beginning on February 15, 2017, InterMountain provided preliminary notice to current direct employees and managed employees of InterMountain client businesses via work-place

announcements. On February 21, 2017, InterMountain will begin providing written notice of this incident to all affected individuals, which includes approximately one (1) New Hampshire resident. Written notice will be provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and to Be Taken

Upon discovering the fraudulent nature of the email, InterMountain moved quickly to identify those that may be affected, to put in place resources to assist them, and to provide them with notice of this incident.

InterMountain is providing all potentially affected individuals access to 2 free years of credit monitoring and identity protection services through AllClear ID, and has established a dedicated hotline for potentially affected individuals to contact with questions or concerns regarding this incident. Additionally, InterMountain is providing potentially impacted individuals with guidance on how to better protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. InterMountain is also providing written notice of this incident to other state regulators as necessary, as well as to the major consumer reporting agencies. InterMountain has provided notice of this incident to the IRS and state tax authorities so that they better monitor for suspicious tax filing activity relating to individuals affected as a result of this incident.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 267-930-4776.

Very truly yours,

Edward J. Finn of
MULLEN COUGHLIN LLC

EJF:ncl
Enclosure

Exhibit A

InterMountain
A business of a thousand details...

Processing Center • P.O. BOX 141578 • Austin, TX 78714

STATE OF NH
DEPT OF JUSTICE
2017 FEB 27 PM 12: 03

00001
ACD1234

00001
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

February 21, 2017

Re: Notice of Data Breach

Dear John Sample:

InterMountain Management, LLC ("InterMountain"), is writing to make you aware of a recent email spoofing attack that may affect the security of your personal information. We take this incident very seriously and are providing you with information and access to resources so that you can protect your personal information, should you feel it is appropriate to do so.

Why Am I Receiving This Notice from InterMountain? You are receiving this notification because InterMountain generated a 2016 IRS Tax Form W-2 for you because either (1) you were directly employed by InterMountain during 2016; OR (2) InterMountain managed the preparation of employee IRS Tax Form W-2s on behalf of an employer you worked for in 2016.

What Happened? We recently discovered that our company was the victim of an email spoofing attack on February 3, 2017, by an individual pretending to be the owner of our company. A request was made for all 2016 W-2 forms prepared by InterMountain. Unfortunately, copies of all 2016 W-2 forms prepared by InterMountain were provided before we discovered that the request was made from a fraudulent account. We discovered the fraudulent nature of the request on February 6, 2017, and have been working tirelessly to investigate and to mitigate the impact of the attack.

What Information Was Involved? A copy of your 2016 IRS Tax Form W-2 was sent in response to the fraudulent email. An IRS Tax Form W-2 includes the following categories of information: (1) the employee's name; (2) the employee's address; (3) the employee's Social Security number; and (4) the employee's wage information. Other than information contained on the 2016 IRS Tax Form W-2, no personal financial information was emailed to the external email account.

What We Are Doing. The confidentiality, privacy, and security of the employee information in our care is one of our highest priorities. InterMountain has stringent security measures in place to protect the security of information in our possession. At this time, we do not believe that the individuals who sent the fraudulent emails accessed our computer network or that our IT systems were otherwise compromised by this attack. We have coordinated with the IRS and state tax authorities so that they can better monitor for tax-related fraud against individuals impacted by this event. We will be providing notice of this incident to certain state regulators, as necessary.

As an added precaution, we have arranged to have AllClear ID protect your identity for 24 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 24 months.

AllClear Identity Repair: You can use this service with no enrollment required. If a problem arises, simply call 1-855-725-5775 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 phone by calling 1-855-725-5775 using the following redemption code: Redemption Code.

Please note: Additional steps may be required by you in order to activate your phone alerts and monitoring options.

The cost of this service will be paid for by InterMountain. ***We strongly encourage you to act to take advantage of these free identity protection services as soon as possible.*** It is incumbent upon you to enroll in these services, as we are not able to act on your behalf to enroll you in the credit monitoring service.

What You Can Do. You can review the enclosed "Steps You Can Take to Prevent Identity Theft and Fraud." You can also enroll to receive the free credit monitoring and identity restoration services described above. In addition, if you have not already done so, we encourage you to file your 2016 tax return as soon as possible. If you have had a fraudulent return filed, you should file the IRS Form 14039, Identity Theft Affidavit, with a paper copy of the return, and mail according to the instructions. A copy of this form can be found at https://www.irs.gov/uac/taxpayer-guide-to-identity-theft.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 1-855-725-5775 (toll free), Monday through Saturday, 9:00 a.m. to 9:00 p.m. ET.

InterMountain takes the privacy and security of the personal information in our care seriously. We sincerely regret any inconvenience or concern this incident has caused you.

Sincerely,

Pam Meador

Pam Meador
Director of Human Resources

STEPS YOU CAN TAKE TO PREVENT IDENTITY THEFT AND FRAUD

While we continue to investigate, you may take direct action to further protect against possible identity theft or financial loss.

We encourage you to file your tax return as soon as possible, if you have not already done so. You can also contact the IRS at www.irs.gov/Individuals/Identity-Protection for helpful information and guidance on steps you can take to prevent a fraudulent tax return from being filed in your name and what to do if you become the victim of such fraud. You can also visit www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information.

You should also look to the information made available by the tax authority for your state of residence and any other state where you file a tax return. For a list of websites for each US state's tax authority, visit http://www.taxadmin.org/state-tax-agencies.

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports and explanation of benefits forms for suspicious activity. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19106
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised 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, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft and you provide the credit bureau with a valid police report, it cannot charge you to place, list, or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze	Experian Security Freeze	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-685-1111	1-888-397-3742	1-888-909-8872
https://www.freeze.equifax.com	www.experian.com/freeze/	www.transunion.com/

You can further educate yourself regarding identity theft, fraud alerts, and the steps you can take to protect yourself, by contacting the Federal Trade Commission or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. **For North Carolina residents**, the Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400; and online at www.ncdoj.gov. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or 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 they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.

InterMountain
A business of a thousand details...
Processing Center • P.O. BOX 141578 • Austin, TX 78714

00001
ACD1234

00001
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

21 de febrero de 2017

Ref.: Notificación de filtración de datos

Estimado John Sample:

InterMountain Management, LLC ("InterMountain"), le escribe para poner en su conocimiento de un ataque reciente al correo electrónico que podría afectar la seguridad de su información personal. Tomamos este incidente con mucha seriedad y le brindamos la información y acceso a recursos para que pueda proteger su información personal, en caso de que considere apropiado hacerlo.

¿Por qué recibo esta notificación de InterMountain? Usted recibe esta notificación porque InterMountain generó un Formulario Impositivo W-2 del IRS para el 2016 a su nombre porque 1) usted era empleado directamente por InterMountain durante el 2016; O 2) InterMountain se ocupó de la preparación del Formulario Impositivo W-2 del IRS en nombre de un empleador para quien usted trabajó en el 2016.

¿Qué sucedió? Recientemente descubrimos que nuestra empresa fue víctima de un ataque al correo electrónico el 3 de febrero de 2017 por un individuo que dijo ser el propietario de nuestra empresa. Se presentó un pedido de todos los formularios W-2 de 2016 preparados por InterMountain. Lamentablemente, copias de todos los formularios W-2 de 2016 preparados por InterMountain fueron provistas antes de descubrir que el pedido fue hecho desde una cuenta fraudulenta. Descubrimos la naturaleza fraudulenta del pedido el 6 de febrero de 2017 y nos hemos ocupado incesantemente para investigar y reducir el impacto del ataque.

¿Qué información resultó involucrada? Una copia de su Formulario Impositivo W-2 del IRS de 2016 fue enviada como respuesta al mensaje electrónico fraudulento. Un Formulario Impositivo W-2 del IRS incluye las siguientes categorías de información: 1) El nombre del empleado; 2) la dirección del empleado; 3) el número de Seguro Social del empleado; y 4) la información sobre los jornales del empleado. Excepto la información contenida en el Formulario Impositivo W-2 del IRS de 2016, no se envió electrónicamente información financiera personal a la cuenta externa de correo electrónico.

¿Qué estamos haciendo? La confidencialidad, privacidad y seguridad de la información del empleado bajo nuestro cuidado es una de nuestras prioridades más importantes. InterMountain ha adoptado estrictas medidas de seguridad para proteger la seguridad de la información en nuestro poder. En este momento, no creemos que los individuos que enviaron los mensajes electrónicos fraudulentos lograron el acceso a nuestra red de computadoras o que nuestros sistemas informáticos fueron de otra manera afectados por este ataque. Hemos coordinado con el IRS y las autoridades impositivas del estado para que puedan monitorizar mejor el fraude impositivo contra los individuos afectados por este evento. Cuando sea necesario, presentaremos información de este incidente a ciertos entes reguladores.

Como precaución adicional, hemos solicitado a AllClear ID que proteja su identidad durante 24 meses sin costo alguno para usted. Los siguientes servicios de protección de la identidad comienzan a partir de la fecha de esta notificación y usted puede usarlos en cualquier momento durante los próximos 24 meses.

AllClear Identity Repair: Usted puede usar este servicio sin que se requiera su inscripción. Si surge un problema, simplemente llame al 1-855-725-5775 y un investigador dedicado le ayudará a recuperar las pérdidas financieras, restaurar su crédito y asegurarse de que su identidad vuelve a su condición apropiada.

AllClear Credit Monitoring: Este servicio ofrece niveles adicionales de protección que incluyen la monitorización del crédito y una póliza de seguro contra el robo de la identidad de un millón de dólares. Para usar este servicio, necesitará proveer su información personal a AllClear ID. Puede inscribirse en línea en enroll.allclearid.com o por teléfono llamando al 1-855-725-5775 usando el siguiente código de rescate: Redemption Code.

Por favor, tome nota: Podrían requerirse pasos adicionales de su parte para activar sus alertas telefónicas y opciones de monitorización.

El costo de este servicio será pagado por InterMountain. ***Nosotros le sugerimos enfáticamente que aproveche estos servicios gratuitos de protección de la identidad lo antes posible.*** Depende de usted inscribirse en estos servicios ya que nosotros no podemos actuar en su nombre para inscribirlo en el servicio de monitorización del crédito.

Qué puede hacer. Puede consultar la publicación adjunta "Pasos que puede tomar para prevenir el robo de identidad y fraude". También puede inscribirse para recibir los servicios gratuitos de monitorización del crédito y restauración de la identidad que se describen más arriba. Además, si todavía no lo ha hecho, le sugerimos que presente su declaración impositiva del 2016 lo antes posible. Si alguien ha presentado una declaración fraudulenta, deberá presentar el Formulario 14039 del IRS, Declaración Jurada de Robo de Identidad, con una copia impresa de la declaración y enviarlo según las instrucciones. Se puede obtener una copia de este formulario en https://www.irs.gov/uac/taxpayer-guide-to-identity-theft.

Para más información. Entendemos que usted podría tener preguntas sobre este incidente que no se incluyen en esta carta. Si tiene preguntas adicionales, por favor llame a nuestra línea de asistencia dedicada al 1-855-725-5775 (gratis), de lunes a sábado, de 9:00 a.m. a 9:00 p.m., hora del este.

InterMountain considera a la privacidad y seguridad de su información personal en nuestro poder con mucha seriedad. Lamentamos con sinceridad cualquier inquietud o inconveniente que este incidente le haya causado.

Atentamente,

Pam Meador

Pam Meador
Directora de Recursos Humanos

PASOS QUE PUEDE TOMAR PARA PREVENIR EL ROBO DE IDENTIDAD Y EL FRAUDE

Mientras continuamos investigando, usted puede tomar medidas directas para protegerse contra el posible robo de identidad y pérdida financiera.

Le sugerimos que presente su declaración impositiva lo antes posible, si todavía no lo ha hecho. También puede comunicarse con el IRS en www.irs.gov/Individuals/Identity-Protection para obtener información útil y guía sobre los pasos que puede tomar para prevenir que se presente una declaración impositiva fraudulenta en su nombre y qué hacer si es víctima de dicho fraude. También puede visitar www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft para más información.

Debe buscar la información puesta a disposición por la autoridad impositiva de su estado de residencia y cualquier otro estado donde presente una declaración impositiva. Para obtener una lista de los sitios web de la autoridad impositiva de cada estado, visite http://www.taxadmin.org/state-tax-agencies.

Le aconsejamos que mantenga la vigilancia contra incidentes de robo de identidad y fraude, que evalúe sus estados de cuenta y que monitorice sus informes crediticios y formularios de explicación de beneficios por actividad sospechosa. Bajo las leyes de EE.UU., usted tiene derecho a un informe crediticio anual gratis de cada una de las tres empresas de informes crediticios más importantes. Para solicitar su informe crediticio gratis, visite www.annualcreditreport.com o llame gratis al 1-877-322-8228. También puede comunicarse directamente con las tres empresas crediticias más importantes para solicitar una copia gratis de su informe crediticio.

Sin cargo, puede pedir que estas empresas de informes crediticios coloquen un "alerta de fraude" a su archivo que alerte a los acreedores a tomar medidas adicionales para verificar su identidad antes de otorgar un crédito a su nombre. Note, sin embargo, que debido a que indica a los acreedores que deben cumplir ciertos procedimientos para protegerlo, también podría retrasar su capacidad de obtener un crédito mientras la agencia verifica su identidad. Ni bien una empresa de informes crediticios confirma su alerta del fraude, las otras son notificadas que deben colocar un alerta del fraude a su archivo. Si desea colocar un alerta del fraude, o tiene alguna pregunta sobre su informe crediticio, por favor comuníquese con una de las tres empresas que aparecen a continuación.

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19106
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

También puede solicitar un congelamiento de sus informes crediticios. Un congelamiento de seguridad prohíbe que la empresa de informes crediticios comparta información del informe de crédito del consumidor sin la autorización escrita del consumidor. Sin embargo, tenga en cuenta que un congelamiento de seguridad a su informe crediticio podría retrasar, interferir o prevenir la aprobación oportuna de cualquier solicitud que presente por créditos nuevos, hipotecas, empleo, vivienda u otros servicios. Si ha sido víctima del robo de identidad y presenta a la empresa de informes crediticios una denuncia policial válida, no puede cobrarle por colocar, listar o levantar un congelamiento de seguridad. En todos los otros casos, la empresa de informes crediticios podrá cobrarle para colocar, cancelar transitoriamente o remover permanentemente un congelamiento de seguridad. Usted necesitará crear un congelamiento de seguridad diferente en cada una de las tres empresas principales de informes crediticios listadas más arriba si desea congelar todos sus archivos de crédito. Para obtener más información sobre cómo crear un congelamiento de seguridad, puede usar la siguiente información de contacto:

Equifax Security Freeze	Experian Security Freeze	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-685-1111	1-888-397-3742	1-888-909-8872
https://www.freeze.equifax.com	www.experian.com/freeze/	www.transunion.com/

También puede educarse sobre el robo de la identidad, las alertas de fraude y las medidas que puede tomar para protegerse, si se comunica con la Comisión Federal de Comercio o el Fiscal General de su estado. Se puede comunicar con la Comisión Federal de Comercio en: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); y por TTY: 1-866-653-4261. **Para residentes de Carolina del Norte**, se pueden comunicar con el Fiscal General por correo al 9001 Mail Service Center, Raleigh, NC 27699-9001; llamando gratis al 1-877-566-7226; por teléfono al 1-919-716-6400; y en línea en www.ncdoj.gov. La Comisión Federal de Comercio también sugiere a quienes descubren que su información ha sido usada equivocadamente que presenten una queja ante ellos. Usted puede obtener información adicional sobre cómo presentar dicha queja a través de la información de contacto que aparece más arriba. Usted tiene el derecho a presentar una denuncia policial si experimenta robo de identidad o fraude. Por favor, note que para poder presentar la denuncia de un crimen o incidente ante las autoridades policiales por robo de identidad, deberá presentar alguna prueba de que ha sido víctima. Las circunstancias de robo de identidad conocida o sospechada también deben ser informadas a las autoridades policiales. Esta notificación no ha sido retrasada por las autoridades policiales.