Melnik Legal PLLC
8710 W. Hillsborough Ave, Ste. 403
Tampa, FL 33615

Tatiana Melnik
Telephone: (734) 358-4201
tatiana@melniklegal.com
http://www.melniklegal.com

VIA U.S. PRIORITY MAIL

February 10, 2019

Attorney General Gordon J. MacDonald
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Security Breach Notification

Dear Attorney General MacDonald:

On behalf of this firm's client, USR Holdings, LLC ("USR") located at 1193 S.E. Port Saint Lucie Blvd., Suite 142, Port Saint Lucie, FL 34952, I write to provide you with notice of a security breach that exposed certain personal information of New Hampshire residents to unauthorized access.

1. **General description of the security breach and steps taken.**

   While performing routine maintenance and backups on December 8, 2018, USR became aware of unusual activity (*i.e.*, missing data) within one server that stored an internally-facing application and database that contained protected health information, some of which was personal information. On December 8, 2018, the database server was taken offline for investigation. During the investigation, USR and a forensic specialist discovered that on August 23, 2018, a USR employee made a configuration change to a firewall rule, which inadvertently allowed the internally-facing database to be available externally from August 23, 2018 until December 8, 2018. This resulted in the database as well as the protected health information and personal information stored in the database being accessed by unauthorized, unknown third parties. The third parties were able to delete the data in the database.

   In response to the breach, USR disabled access to the database server and engaged a national digital forensics firm to assist with the investigation. In addition, USR is providing additional staff training and is revisiting its security measures to reduce the likelihood of a similar incident in the future. Also, as discussed further below, each affected New Hampshire resident is being offered credit monitoring and identity theft protection services.

2. **Types of personal information that were compromised or are reasonably believed to have been compromised as a result of the breach.**

   The database contained information for 223 New Hampshire residents. The database included names, addresses (for some), dates of birth, and insurance information for the individuals. In some circumstances, the insurance information included the name of the carrier, the member id, the name of the primary insured, deductible amount and amount remaining, address of the primary insured, the relationship between the primary insured and the individual, and similar benefits information.

   For three of the individuals, the social security number was included.

   The database did not include any of the following: driver's license number or government identification number, credit or debit card number, or financial account number.

3. **Notice to New Hampshire residents and credit monitoring.**

   USR engaged ID Experts® to assist with notification. USR mailed notifications through ID Experts on February 1, 2019. A copy of the notification template is enclosed.

Credit monitoring and identity theft protection services are being offered through ID Experts® to all affected individuals. These services include credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services, including access to ID Experts' Member Services' team Monday through Friday from 8 am - 8 pm Eastern Time.

Should you have any questions regarding this notification, you may reach me directly by phone at (734) 358-4201 or by e-mail at tatiana@melniklegal.com.

Very truly yours,

Melnik Legal PLLC

Tatiana Melnik

Enclosure

To Enroll, Please Call:
(800) 961-7033
Or Visit:
https://app.myidcare.com/account-creation/protect
Enrollment Code: <<XXXXXXX>>

C/O ID Experts
PO Box 10444
Dublin, OH 43017-4044

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

February 1, 2019

Dear <<First Name>> <<Last Name>>:

We are writing to inform you of a recent data security breach experienced by USR Holdings, LLC ("USR") that impacted Amethyst Recovery Center, LLC, The Freedom Center, LLC, and New England Recovery and Wellness, LLC (each referred to in this Letter as the "Center"). As a result of this breach, personal health information belonging to you or a family member may have been compromised. We have no indication that any information has been misused in any way. Most importantly, we want to apologize; we understand how important your privacy is to you and take this matter very seriously.

What Happened?

On December 8, 2018, USR became aware of unusual activity within one USR server, which stored data for the Center. The server contained personal information about you or your family member. We immediately disabled access to the server and launched an investigation to determine what happened and the extent of the incident. With help from a national digital forensics firm, our investigation determined that on August 23, 2018, a USR staff member made a configuration change to a firewall that resulted in your information on the server being accessed by unauthorized, unknown third parties.

What Information Was Involved?

While the information present in the database varies by individual, the third parties may have accessed demographic data and health insurance information about you or your family member, including your or your family member's first and last name, date of birth, address, health insurance subscriber number, and in some very limited instances, a social security number. **Importantly, the database did not include any admissions records, treatment records, bank account information, or credit card information.**

What We Are Doing:

We are taking proactive steps to limit the impact of this incident and to help mitigate the potential for harm, including disabling access to the server and engaging a national digital forensics firm to assist with the investigation. In addition, we are providing additional staff training and are revisiting our security measures to reduce the likelihood of a similar incident in the future. Finally, we are reporting this incident to the appropriate authorities, including the U.S. Department of Health and Human Services Office for Civil Rights.

As an added precaution to help protect your information from potential misuse, we are also offering you identity theft protection services through ID Experts®, the data breach and recovery services expert, to provide you with MyIDCare™. MyIDCare services include: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services, including access to ID Experts' Member Services' team.

What You Can Do:

We encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling (800) 961-7033 or going to https://app.myidcare.com/account-creation/protect and using the Enrollment Code provided above. MyIDCare experts are available Monday through Friday from 8 am - 8 pm Eastern Time. **Please note the deadline to enroll is May 2, 2019**.

While we are unaware of any actual or attempted misuse of your information as a result of this event, we nevertheless encourage you to remain vigilant by reviewing your health insurance account records, explanation of benefits forms, and credit reports and immediately reporting all suspicious activity to the institution that issued the record. Please also review the "Additional Resources and Information" section included with this letter. This section describes additional steps you can take to help protect yourself, including details on how to place a fraud alert or a security freeze on your credit file and how to obtain a free copy of your credit report. You may also contact the MyIDCare representatives, who can answer questions or concerns you may have regarding the protection of your personal information.

For More Information:

You will find detailed instructions for enrollment on the enclosed "Additional Resources and Information" document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call (800) 961-7033 or go to https://app.myidcare.com/account-creation/protect for assistance or for any additional questions you may have.

We sincerely apologize for any inconvenience or concern this incident has caused, and we encourage you to reach out to us with any questions you may have.

Very truly yours,

USR Holdings, LLC

Enclosures

ADDITIONAL RESOURCES AND INFORMATION

MyIDCare™.

1. **Website and Enrollment.** Go to https://app.myidcare.com/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.
2. **Activate the credit monitoring** provided as part of your MyIDCare membership. **The monitoring included in the membership must be activated to be effective**. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, MyIDCare will be able to assist you.
3. **Telephone.** Contact MyIDCare at (800) 961-7033 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

Free Credit Report. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports for unauthorized activity. Under federal law, you may obtain a copy of your credit report, free of charge, once every 12 months from each of the three credit reporting companies. To order your free credit report, please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

Fraud Alerts. You may place a fraud alert in your file by calling one of the nationwide credit reporting bureaus listed below. 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 may also delay you when you seek to obtain credit. 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.

Security Freezes. In some U.S. states, you have the ability to place a security freeze on your credit report. By placing a security 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 **each** of the three national credit reporting bureaus listed above 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.

To learn more about how to prevent identity theft, including the use of fraud alerts and security freezes, you can contact the Federal Trade Commission, or the nationwide credit reporting agencies at the contact information listed below.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, DC 20580, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261, www.consumer.ftc.gov.

Maryland Residents: 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023 (toll free when calling within Maryland) (410) 576-6300 (for calls originating outside Maryland).

Rhode Island Residents: 150 South Main Street, Providence, RI 02903, www.riag.ri.gov, 401- 274-4400

Report Fraudulent Activity. If you discover any suspicious items in your credit report, believe that you are the victim of identity theft, or have reason to believe that your personal information has been misused, and you have enrolled in MyIDCare, notify them immediately by calling or by logging into the MyIDCare website and filing a request for help. If you file a request for help or report suspicious activity, you will be contacted by a member of the MyIDCare team who will help you determine the cause of the suspicious items.

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 or to the Attorney General.

Contact the Nationwide Credit Reporting Agencies.

	Fraud Alert	**Security Freeze**
Equifax P.O. Box 105788 Atlanta, GA 30348	By Phone: 1-888-766-0008 Online: www.alerts.equifax.com	By Phone: 1-800-349-9960 Online: www.freeze.equifax.com
Experian P.O. Box 9554 Allen, TX 75013	By Phone: 1-888-397-3742 Online: www.experian.com	By Phone: 1-888-397-3742 Online: www.experian.com/freeze
TransUnion P.O. Box 2000 Chester, PA 19022	By Phone: 1-888-909-8872 Online: www.transunion.com	By Phone: 1-800-680-7289 Online: www.transunion.com/credit-freeze

You also have certain rights under the Fair Credit Reporting Act (FCRA), including: to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA and ways to obtain a free credit report, please visit https://www.consumer.ftc.gov/articles/0155-free-credit-reports.

What do I do if my family member is deceased? You may contact the credit bureaus listed above, and request they flag your family member's credit file. This will prevent the credit file information from being used to open credit. You may be required to mail a copy of your family member's death certificate to each company.