



Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

RE: Notice of Data Breach

Dear <<Name1>>:

The National Registry of Emergency Medical Technicians (“NREMT”) is writing to inform you of a recent incident that may impact the security of your personal information. This letter contains details about the incident and our response, as well as steps you can take to protect your information, should you feel it appropriate to do so.

What Happened? As part of the NREMT certification process, NREMT works collaboratively with the Nevada Department of Health and Human Services (“NDHHS”). On December 14, 2017, NREMT learned that credentials belonging to a NDHHS employee were used without authorization on the NREMT certification web-based platform. NREMT immediately changed the account credentials and launched an internal investigation to determine the nature and scope of this event, including retaining the services of a third party forensic investigation firm to assist with their own internal investigation. Although the investigation is ongoing, NREMT determined the NDHHS employee’s credentials were impermissibly used by an unknown person or persons, beginning on November 17, 2017, to mark candidates as “Exam Complete” although they had not yet completed the EMT examination process. This impermissible use may have compromised the candidates’ personal information, including Social Security numbers.

What Information was Involved? While our investigation is ongoing, we determined on January 9, 2018, that the following information related to you may have been accessible to the unauthorized individual(s): first and last name, address information, and Social Security number. Financial account data was not affected in this incident.

What We Are Doing. The confidentiality, privacy, and security of information in our care is one of our highest priorities. When we discovered this incident, we immediately took steps to terminate the unauthorized access, determine how this event occurred, and confirm what personal data may have been at risk as a result of this incident. We are also working with NDHHS to validate all EMT candidate certifications as legitimate. In addition to providing this notice to you and access to free credit monitoring and identity theft recovery services, we have been working with our third-party forensic investigation team to ensure the security of our systems and to prevent something like this from happening again. We provided notice of this event to the FBI and will also be providing notice to your state officials and consumer reporting agencies as required.

What You Can Do. You can review the enclosed *Steps You Can Take to Protect Against Identity Theft and Fraud*, which contains instructions on how to enroll and receive free credit monitoring and identity restoration services, as well as information on what you can do to better protect yourself against the possibility of identity theft and fraud should you feel it is appropriate to do so.

For More Information. We sincerely regret any inconvenience or concern this may have caused. We understand you may have questions that are not answered in this letter. To insure your questions are answered in a timely manner, please contact Epiq Systems at 844-659-0623, Monday through Friday from 6:00 a.m. to 6:00 p.m. Pacific Standard Time.

Sincerely,

A handwritten signature in cursive script that reads "Drew E Dawson".

Drew Dawson
Interim Executive Director

Encl.

Steps You Can Take to Protect Against Identity Theft and Fraud

As an added precaution, we have arranged for you to enroll, at no cost to you, in an online three-bureau credit monitoring service (*myTrueIdentity*) for one year provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go to the *myTrueIdentity* website at www.mytrueidentity.com and in the space referenced as “Enter Activation Code”, enter the following unique 12-letter Activation Code <<Enrollment Code>> and follow the three steps to receive your credit monitoring service online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper based, three-bureau credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the following 6-digit telephone pass code <<Engagement Code>> and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score. The daily three-bureau credit monitoring service will notify you if there are any critical changes to your credit files at TransUnion®, Experian® and Equifax®, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes access to an identity restoration program that provides assistance in the event your identity is compromised to help you restore your identity and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

You can sign up for the online or offline credit monitoring service anytime between now and <<Enrollment Deadline>>. Due to privacy laws, we cannot register you directly. Please note that credit monitoring and identity restoration services might not be available for individuals who do not have a credit file with TransUnion, or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score. The identity restoration assistance is available to you for one year from the date of this letter with no enrollment required. If you believe you may be a victim of identity theft please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the following 6-digit telephone pass code <<Engagement Code>> to speak to a dedicated TransUnion representative about your identity theft issue.

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports 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
P.O. Box 105069
Atlanta, GA 30348
800-525-6285
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19022-2000
800-680-7289
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

P.O. Box 105788
Atlanta, GA 30348
1-800-685-1111

<https://www.freeze.equifax.com>

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/freeze/center.html

TransUnion

P.O. Box 2000
Chester, PA 19022-2000
1-888-909-8872

www.transunion.com/credit-freeze

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. 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. **For Maryland residents**, the Attorney General can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us. **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. **For Rhode Island residents**, the Attorney General can be contacted by mail at 150 South Main Street, Providence, RI 02903; by phone at (401) 274-4400; and online at www.riag.ri.gov. A total of 0 Rhode Island resident(s) may be impacted by this incident. **For New Mexico residents**, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580. 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.



Return Mail Processing Center
 PO Box 6336
 Portland, OR 97228-6336

<<Mail ID>>
 To the Parent or Guardian of
 <<Name 1>>
 <<Name 2>>
 <<Address 1>>
 <<Address 2>>
 <<Address 3>>
 <<Address 4>>
 <<Address 5>>
 <<City>><<State>><<Zip>>
 <<Country>>

<<Date>>

RE: Notice of Data Breach

To the Parent or Guardian of <<Name1>>:

The National Registry of Emergency Medical Technicians (“NREMT”) is writing to inform you of a recent incident that may impact the security of your minor’s personal information. This letter contains details about the incident and our response, as well as steps you can take to protect your minor’s information, should you feel it appropriate to do so.

What Happened? As part of the NREMT certification process, NREMT works collaboratively with the Nevada Department of Health and Human Services (“NDHHS”). On December 14, 2017, NREMT learned that credentials belonging to a NDHHS employee were used without authorization on the NREMT certification web-based platform. NREMT immediately changed the account credentials and launched an internal investigation to determine the nature and scope of this event, including retaining the services of a third party forensic investigation firm to assist with their own internal investigation. Although the investigation is ongoing, NREMT determined the NDHHS employee’s credentials were impermissibly used by an unknown person or persons, beginning on November 17, 2017, to mark candidates as “Exam Complete” although they had not yet completed the EMT examination process. This impermissible use may have compromised the candidates’ personal information, including Social Security numbers.

What Information was Involved? While our investigation is ongoing, we determined on January 9, 2018, that the following information related to your minor may have been accessible to the unauthorized individual(s): first and last name, address information, and Social Security number. Financial account data was not affected in this incident.

What We Are Doing. The confidentiality, privacy, and security of information in our care is one of our highest priorities. When we discovered this incident, we immediately took steps to terminate the unauthorized access, determine how this event occurred, and confirm what personal data may have been at risk as a result of this incident. We are also working with NDHHS to validate all EMT candidate certifications as legitimate. In addition to providing this notice to you and access to free identity theft recovery services, we have been working with our third-party forensic investigation team to ensure the security of our systems and to prevent something like this from happening again. We provided notice of this event to the FBI and will also be providing notice to your state officials and consumer reporting agencies as required.

What You Can Do. You can review the enclosed *Steps You Can Take to Protect Against Identity Theft and Fraud*, which contains instructions on how to enroll and receive free identity restoration services for your minor, as well as information on what you can do to better protect your minor against the possibility of identity theft and fraud should you feel it is appropriate to do so.

For More Information. We sincerely regret any inconvenience or concern this may have caused. We understand you may have questions that are not answered in this letter. To insure your questions are answered in a timely manner, please contact Epiq Systems at 844-659-0623, Monday through Friday from 6:00 a.m. to 6:00 p.m. Pacific Standard Time.

Sincerely,

A handwritten signature in cursive script that reads "Drew E Dawson".

Drew Dawson
Interim Executive Director

Encl.

Steps You Can Take to Protect Against Identity Theft and Fraud

As an added precaution, we recommend you visit TransUnion's secure online form at www.transunion.com/childidentitytheft to submit your minor's information so TransUnion can check their database for a credit file with your minor's Social Security Number. After TransUnion's search is complete, they will respond to you at the email address you provide. If they locate a file in your minor's name, they will ask you for additional information in order to proceed with steps to protect your minor from any impact associated with this fraudulent activity.

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your minor's account statements, and to monitor your minor's credit reports for suspicious activity. Typically, credit is not granted to individuals under the age of 18 and, therefore, the credit bureaus may not maintain a credit file on your minor. Under U.S. law you are entitled to one free credit report, if one exists, 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 minor's credit report.

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

Equifax
P.O. Box 105069
Atlanta, GA 30348
800-525-6285
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19022-2000
800-680-7289
www.transunion.com

You may also place a security freeze on your minor's credit reports, if such reports exist. 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 minor's credit report may delay, interfere with, or prevent the timely approval of any requests your minor makes for new loans, credit mortgages, employment, housing, or other services. If your minor is 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 minor's credit files, if such files exist. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-685-1111
<https://www.freeze.equifax.com>

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
P.O. Box 2000
Chester, PA 19022-2000
1-888-909-8872
www.transunion.com/credit-freeze

You can further educate yourself regarding identity theft, fraud alerts and security freezes, and the steps you can take to protect yourself and your minor, by contacting the Federal Trade Commission or your state Attorney General. 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.