150 N. Riverside Plaza, Suite 3000, Chicago, IL 60606 • (312) 819-1900

July 12, 2019

Bruce A. Radke

312-463-6211
312-819-1910
bradke@polsinelli.com

VIA E-MAIL (ATTORNEYGENERAL@DOJ.NH.GOV)
AND FEDERAL EXPRESS

The Honorable Gordon MacDonald
Attorney General of the State of New Hampshire
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notification of a Data Security Incident

Dear Attorney General MacDonald:

We represent Sophia Snow House, Inc. ("Sophia Snow House"), in connection with an incident that involved the personal information of one (1) New Hampshire resident and provide this notice on behalf of Sophia Snow House pursuant to N.H. REV. STAT. ANN. § 359-C:20.

This notice will be supplemented, if necessary, with any new significant facts discovered subsequent to its submission. While Sophia Snow House is notifying you of this incident, Sophia Snow House does not waive any rights or defenses relating to the incident or this notice, or the applicability of New Hampshire law on personal jurisdiction.

NATURE OF THE SECURITY BREACH OR UNAUTHORIZED USE OR ACCESS

TenX Systems, LLC d/b/a ResiDex Software ("ResiDex") assists Sophia Snow House in managing certain information about Sophia Snow House's residents. ResiDex notified Sophia Snow House that ResiDex experienced a data security incident involving ransomware. ResiDex's forensic investigation was unable to rule out the possibility that personal information was subject to unauthorized access and potential exfiltration from the ResiDex servers as a result of the incident due to the complexity of the event and efforts undertaken by the perpetrators to conceal their actions. ResiDex's investigation determined that first access to ResiDex's systems occurred on approximately April 2, 2019, with the ransomware executed on April 9, 2019. The data security incident may have resulted in unauthorized access to personal information that

existed on ResiDex's system as of April 9, 2019, including names, Social Security numbers, and medical information.

NUMBER OF NEW HAMPSHIRE RESIDENTS AFFECTED

On May 29, 2019, Sophia Snow House determined that one (1) New Hampshire resident may have been impacted by this incident. Sophia Snow House is notifying the impacted resident of the situation by letter today, July 12, 2019. The notification letter will include an offer for complimentary credit monitoring and identity theft protection. Enclosed is a copy of the notice that is being sent to the impacted resident via first-class United States mail.

STEPS TAKEN RELATING TO THE INCIDENT

Upon learning of the incident, Sophia Snow House coordinated with ResiDex to investigate the incident. ResiDex has represented to Sophia Snow House that ResiDex has taken steps to further secure its information systems to prevent a similar incident from occurring in the future. Finally, as discussed above, Sophia Snow House is notifying impacted individuals and providing them with information on how they can protect themselves against fraudulent activity and identity theft.

CONTACT INFORMATION

Please contact me if you have any questions or if I can provide you with any further information concerning this matter.

Very truly yours,

Bruce A. Radke

Enclosure

TenX Systems, LLC d/b/a ResiDex Software
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>>

Dear <<Name 1>>:

NOTICE OF DATA BREACH

TenX Systems, LLC d/b/a ResiDex Software ("ResiDex") specializes in providing software for assisted living homes, group homes, and organizations providing care for the elderly or disabled, including <<Variable 1>>. ResiDex understands the importance of protecting your personal information and protected health information. We are writing to inform you that we recently identified and addressed a security incident that may have involved your personal information and/or protected health information. This notice describes the incident, outlines the measures we have taken in response, and advises you on steps you can take to further protect your information.

What Happened?

On April 9, 2019, ResiDex became aware of a data security incident, including ransomware, which impacted our server infrastructure and took our systems offline. ResiDex immediately undertook efforts to restore its servers to a new hosting provider. Backups and other information maintained by ResiDex were used to enable near seamless restoration of security and services on the same day. Additionally, ResiDex took affirmative steps to further safeguard its software systems. ResiDex simultaneously retained a forensic investigation firm to determine the nature of the security compromise and identify any individuals whose personal information and/or protected health information may have been compromised.

What Information Was Involved?

The forensic investigation was unable to identify specific individuals whose personal information and/or protected health information may have been compromised due to the complexity of the event and efforts undertaken by the perpetrators to conceal their actions. The investigation did determine that first access to ResiDex's systems occurred on approximately April 2, 2019, with the ransomware launched on April 9, 2019.

The data security incident may have resulted in unauthorized access to protected health information, including medical records that existed on ResiDex's software as of April 9, 2019, and/or personal information including names and Social Security numbers. Please note that it is entirely possible that your personal information and/or protected health information may not have been compromised as a result of the incident. Nonetheless, we are providing you with this notification in an abundance of caution.

What We Are Doing

As stated above, following the data security incident, ResiDex immediately undertook efforts to restore its servers to a new hosting provider. Backups and other information maintained by ResiDex were used to enable near seamless restoration of security and services on the same day. Additionally, ResiDex took affirmative steps to further safeguard the ResiDex software systems. ResiDex has retained a forensic investigation firm to thoroughly investigate the incident and is providing this notice to you in accordance with applicable state law and Health Insurance Portability and Accountability Act (HIPAA) requirements. Please be advised that ResiDex is continuing to work closely with leading security experts to identify and implement measures to further strengthen the security of their systems to help prevent this from happening in the future.

Additionally, we are offering you a free <<12 or 24>>-month membership to TransUnion *my*TrueIdentity credit monitoring service. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. This product also includes various features such as up to $1,000,000 in identity theft insurance with no deductible, subject to policy limitations and exclusions. TransUnion *my*TrueIdentity is completely free to you and enrolling in this program will not hurt your credit score. For more information on identity theft protection and TransUnion *my*TrueIdentity, including instructions on how to activate your complimentary <<12 or 24>>-month membership, please see the additional information attached to this letter. ***To take advantage of this offer, you must enroll by <<Enrollment Date>>.***

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 <<12-letter Activation 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, 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 <<6 Digit Phone 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.

You can sign up for the online or offline credit monitoring service anytime between now and <<Enrollment Date>>. Due to privacy laws, we cannot register you directly. Please note that credit monitoring 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.

Once you are enrolled, you will be able to obtain <<12 or 24>> months of unlimited access to your TransUnion credit report and credit score. The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, 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.)

What You Can Do

We are aware of how important your personal information and protected health information is to you. To protect yourself from potential harm associated with this incident, we encourage you to closely monitor all mail or other contact from individuals not known to you personally, and avoid answering questions or providing additional information to those individuals. We also ask that you report any such activity, or any suspicious contact whatsoever, to ResiDex as well as to law enforcement if warranted.

We also remind you to remain vigilant for incidents of fraud or identity theft by reviewing account statements and credit reports for unauthorized activity. Residents of the United States are entitled to one free credit report annually from each of the three major credit reporting agencies. To order your free credit reports, visit www.annualcreditreport.com or call toll-free (877) 322-8228. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission.

You may want to consider placing a fraud alert on your credit report. There are two types of fraud alerts 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 alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. A fraud alert does not impact your ability to get a loan or credit, but rather alerts a business that your personal information may have been compromised and requires the business to verify your identity before issuing you credit. Although this may cause some delay if you are applying for credit, it may protect against someone else obtaining credit in your name. 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 contacting any of the three national credit reporting agencies. The agency that you contacted must notify the other two agencies.

Additionally, you have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, 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 security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to access your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit. There is no fee to place or lift a security freeze. However, unlike a fraud alert, you must separately place a security freeze on your credit file at each of the three national credit reporting agencies. To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies by regular, certified or overnight mail at the addresses below or, if available, comply with the consumer reporting agencies' online security freeze request procedures.

In order to request a security freeze, you may need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); and
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

Below are the toll-free numbers and addresses for the three largest credit reporting agencies for purposes of ordering a copy of your credit report:

Equifax	Experian	TransUnion
1-866-349-5191	1-888-397-3742	1-800-888-4213
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	P.O. Box 9554	P.O. Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016

Below are the toll-free numbers and addresses for the three largest credit reporting agencies for purposes of placing a security freeze on your credit file:

Equifax Security Freeze	Experian Security Freeze	TransUnion Security Freeze
1-800-349-9960	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094

Other Important Information

Below is the toll-free number, address and website address for the Federal Trade Commission, which you may contact to obtain further information on how to protect yourself from identity theft and how to repair identity theft:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft

For residents of Iowa: Iowa residents can contact the Office of the Attorney general to obtain information about steps to take to avoid identity theft from the Iowa Attorney General's office at: Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines IA 50319, 515-281-5164.

For residents of Maryland: Maryland residents can contact the Office of the Attorney General to obtain information about steps you can take to avoid identity theft from the Maryland Attorney General's office at: Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, (888) 743-0023, www.oag.state.md.us.

For residents of Rhode Island: We believe that this incident affected 223 Rhode Island residents. Rhode Island residents can contact the Office of the Attorney general at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. You have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For residents of North Carolina: North Carolina residents can obtain information about preventing identity theft from the North Carolina Attorney General's Office at: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov.

For residents of Massachusetts: Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. Massachusetts law also allows consumers to place a security freeze on their credit reports. A security freeze can be placed without any charge.

For More Information

ResiDex and <<Variable 1>> understand the importance of protecting your personal information, and deeply regret any concern this may have caused to you. ResiDex remains committed to protecting your personal information and personal health information. **Should you have any questions and would like further information regarding the information contained in this letter, please do not hesitate to contact 877-347-0184 between 9:00 a.m. to 9:00 p.m. Eastern Time, Monday through Friday.**

Sincerely,

Alex Berg
Privacy Officer, TenX Systems, LLC d/b/a ResiDex Software