

JOSEPH SALVO
JSALVO@GRSM.COM

GORDON & REES
SCULLY MANSUKHANI
YOUR 50 STATE PARTNER™

ATTORNEYS AT LAW
1 BATTERY PARK PLAZA, 28TH FLOOR
NEW YORK, NY 10004
WWW.GRSM.COM

June 19, 2019

VIA ELECTRONIC MAIL (CONSUMER@AG.IOWA.GOV)

Tom Miller, Attorney General
Office of the Attorney General of Iowa
Consumer Protection Division
Security Breach Notifications
Hoover State Office Building
1305 E. Walnut Street
Des Moines, Iowa 50319-0106

Re: Notification of Data Security Incident
Our File No: 1185048

Dear Attorney General Miller:

Our client, 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. ResiDex understands the importance of protecting the personal information provided by its customers and is making this notification to your Office in accordance with applicable law following a recent data security incident.

ResiDex provides software services to various covered entities throughout the country. In accordance with the Health Insurance Portability and Accountability Act (“HIPAA”), certain covered entities have delegated their notification obligations to ResiDex, as its business associate, and ResiDex has provided the notifications to the potentially impacted individuals and is providing this notification to you on the covered entity’s behalf. The covered entities who have delegated notification obligations to ResiDex for purposes of this notification letter are:

- Presbyterian Homes and Services, located across MN, WI, and IA
- Village Ridge, Village Place and Autumn Point, located in Marion, IA and Fort Calhoun, NE

On April 9, 2019, ResiDex became aware of a data security incident, including ransomware, which impacted its server infrastructure and took its 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

June 19, 2019

Page 2

nature of the security compromise and identify any individuals whose personal information and/or protected health information may have been compromised.

The forensic investigation was unable to identify any 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 an individual's personal information and/or protected health information may not have been compromised as a result of the incident.

Nonetheless, ResiDex, at the request of the covered entities, has provided notification to the potentially impacted individuals *via* written and substitute notice beginning on June 7, 2019 in an abundance of caution. A summary of the potentially impacted residents as set forth below:

- Presbyterian Homes and Services, 812 current IA residents
- Village Ridge, Village Place and Autumn Point, 802 current IA residents

A sample copy of the notification to the Iowa residents is attached. As noted in the attachment, ResiDex has included in the notification an offer to provide twelve months of one-bureau credit monitoring services to the affected Iowa residents. ResiDex has also provided notification of this data security incident to the Department of Health and Human Services/Office of Civil Rights on the covered entities' behalf in accordance with HIPAA.

ResiDex is continuing to work closely with leading security experts to identify and implement measures to further strengthen the security of its system to help prevent this from happening in the future.

Best regards,

GORDON REES SCULLY MANSUKHANI, LLP

/s/ Joseph Salvo

Joseph Salvo, Esq.

Enclosures

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>>:

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>> (“Facility”). At the request of the Facility, ResiDex is sending you this notice because you are a current, former or prospective resident of the Facility, or a current or former staff member at the Facility. ResiDex and the Facility understand the importance of protecting your personal information and protected health information. We are writing to inform you that ResiDex 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 that ResiDex has 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 any 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 *myTrueIdentity* 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 *myTrueIdentity* 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 *myTrueIdentity*, including instructions on how to activate your complimentary <<12 or 24 >>-month membership, please see the additional information below. *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 to avoid answering questions or providing additional information to such unknown individuals. We also ask that you report any such activity, or any suspicious contact whatsoever, to the Facility and/or ResiDex, as well as to law enforcement if warranted.

Under the Health Insurance Portability and Accountability Act, we advise you that protected health information is defined as individually identifiable information transmitted or maintained in electronic media or any other form or medium, including demographic information collected from an individual, and relates to the past, present, or future physical or mental health conditions, provision of health care, or payment for health care to an individual.

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.

Below are the toll-free numbers and addresses for the three largest credit reporting agencies:

Equifax
P.O. Box 74021
Atlanta, GA 30374
1-800-685-1111
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

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 Hawaii, Michigan, Missouri, North Carolina, Vermont, and Virginia: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon and West Virginia: It is required by state law to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report using the contact information listed above.

For residents of Iowa: State law advises you to report any suspected identity theft to law enforcement or the Attorney General.

For residents of Oregon: State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Illinois, Maryland, North Carolina, and Rhode Island: You can obtain information from the Offices of the Attorney General in your state and from the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

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

Rhode Island Office of the Attorney General
Consumer Protection
150 South Main Street
Providence, RI 02903
1-401-274-4400
www.riag.ri.gov

Office of the Illinois Attorney General
Identity Theft Hotline
100 W Randolph St, Fl. 12
Chicago, IL 60601
1-866-999-5630
www.illinoisattorneygeneral.gov

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

For residents of Massachusetts and Rhode Island: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of Connecticut, Massachusetts, Rhode Island and West Virginia: You also have the right to place a security freeze on your credit report by contacting any of the credit bureaus listed above.

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.** In the event that the call-in center is unable to assist with your questions, we invite you to contact <<Variable 1>> directly at <<Variable 2>>, or ResiDex directly at (866) 512-8369.

Sincerely,

A handwritten signature in black ink that reads "Alexander Berg". The signature is written in a cursive style with a large initial "A".

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