

RECEIVED
OCT 04 2019
CONSUMER PROTECTION

September 27, 2019

William Sanders
214-698-8063 (direct)
William.Sanders@wilsonelser.com

Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03302

Re: Data Security Incident

Dear Attorney General MacDonald:

We represent Wise Health System with respect to an incident involving the potential exposure of certain personal information described in detail below.

1. Nature of the possible security breach or unauthorized use or access

On March 14, 2019, an email phishing campaign was launched against Wise Health System. Unfortunately, a few of Wise Health System's employees provided their usernames and passwords in response to this phishing email. Once these usernames and passwords were obtained, the intruders used the information to access the Employee Kiosk in an attempt to divert payroll direct deposits. Although we do not believe that it was the intent of the phishing emails to obtain patient information, access to the email boxes may have compromised patient information such as patient medical record number, diagnostic and treatment information, and potentially insurance information. Again, we believe the purpose of this campaign was to divert payroll direct deposits rather than to obtain patient information. Wise Health System has not received any reports of patient identity theft since the date of the phishing incident (March 14, 2019 to present).

2. Number of New Hampshire residents potentially affected

Two (2) New Hampshire residents were affected in this potential incident. New Hampshire is sending the potentially impacted individuals a letter notifying them of this incident. A copy of the notification sent to the potentially impacted individuals is included with this letter, which informs the New Hampshire residents about the 12 months of credit monitoring and identity theft protection services that is being offered to them.

Notification to the impacted New Hampshire residents was sent on September 12, 2019.

3. Steps Wise Health System has taken or plans to take relating to the potential incident

Wise Health System has taken steps to prevent a similar event from occurring in the future, including reviewing its information, security policies and procedures, and implementing additional safeguards to protect against similar threats. Wise Health System also conducted a forensic investigation into the incident and reported the matter to law enforcement.

4. Other notification and contact information

If you have any additional questions, please contact me at William.Sanders@wilsonelser.com or (214) 698-8063.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

/s/ William Sanders

William Sanders



C/O ID Experts
PO Box 4219
Everett WA 98204

ENDORSE



1 NAME
ADDRESS1
ADDRESS2
CSZ
SEQ
CODE 2D

BREAK

To Enroll, Please Call:
833-297-6406
Or Visit:
<https://ide.myidcare.com/wisehealthsystem>
Enrollment Code:
<<XXXXXXXXXX>>

September 12, 2019

Notice of Data Breach

Dear <<FULL NAME>>,

We are writing in order to inform you of an incident that may have exposed your sensitive medical information. We take the security of your personal information seriously and want to provide you with information and resources you can use to protect your information.

What Happened and What Information was Involved?:

On March 14, 2019, an email phishing campaign was launched against Wise Health System. Unfortunately, a few of Wise Health System’s employees provided their usernames and passwords in response to this phishing email. Once these usernames and passwords were obtained, the intruders used the information to access the Employee Kiosk in an attempt to divert payroll direct deposits. Although we do not believe that it was the intent of the phishing emails to obtain patient information, access to the email boxes may have compromised your patient information such as your medical record number, diagnostic and treatment information, and potentially insurance information. Again, we believe the purpose of this campaign was to divert payroll direct deposits rather than to obtain patient information. However, we felt it would be prudent to make you aware of this incident. Wise Health System has not received any reports of patient identity theft since the date of the phishing incident (March 14, 2019 to present).

What We Are Doing:

In light of this incident, we have taken steps to prevent this from happening in the future, including reviewing and altering our security policies and procedures. We have also engaged forensic computer experts to investigate the incident and have reported the matter to law enforcement. We apologize for any inconvenience this may have caused.

We value the safety of your personal information and are therefore offering 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. With this protection, MyIDCare will help you resolve issues if your identity is compromised.

What You Can Do:

We encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling 833-297-6406 or going to <https://ide.myidcare.com/wisehealthsystem> and using the Enrollment Code provided above. MyIDCare experts are available Monday through Friday from 6 am - 6 pm Pacific Time. Please note the deadline to enroll is December 12, 2019.

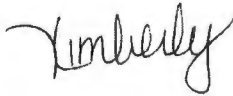
Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. MyIDCare representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information:

You will find detailed instructions for enrollment on the enclosed Recommended Steps 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 833-297-6406 or go to <https://ide.myidcare.com/wishealthsystem> for assistance or for any additional questions you may have.

Sincerely,



Kimberly Browder
Vice President of Compliance & Privacy
System-wide Privacy Officer

(Enclosure)

Additional Important Information

For residents of Hawaii, Michigan, Missouri, Virginia, Vermont, and North Carolina: 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 laws 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 from each of the three nationwide credit reporting agencies. 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 at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of Iowa:

State law advises you to report any suspected identity theft to law enforcement or to 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 Maryland, Rhode Island, Illinois, and North Carolina:

You can obtain information from the Maryland and North Carolina Offices of the Attorneys General and 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

**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

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

For residents of Massachusetts: 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 all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. 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 also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The contact information for all three credit bureaus is below:

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, or regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a freeze. You may obtain a security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
www.freeze.equifax.com
800-525-6285

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

TransUnion (FVAD)
P.O. Box 2000
Chester, PA 19022
freeze.transunion.com
800-680-7289

More information can also be obtained by contacting the Federal Trade Commission listed above.