STINSON

David Axtell
PARTNER
DIRECT: 612.335.7247
OFFICE: 612.335.1500
david.axtell@stinson.com

May 8, 2020

Attorney General Wayne Stenehjem
Office of the Attorney General
600 East Boulevard Ave., Dept 125
Bismarck, ND 58505-0040
E-mail: ndag@nd.gov

Re: Notification of Data Security Incident

Dear Attorney General Wayne Stenehjem:

This firm represents Riverwood Healthcare Center ("Riverwood") located in Minnesota. We are writing to tell you about a data security incident involving our client, Riverwood, that occurred at our client's vendor, Paperless Pay, which provides a service that allows Riverwood employees to view their pay stubs and W2 forms online. While we do not know that personal information was obtained by anyone due to this incident, out of an abundance of caution we are providing this notice. Riverwood takes the protection and proper use of employee information very seriously. For this reason, we are contacting you directly to explain the circumstances of the incident and we are providing information regarding notices and services given to consumers of the breach. According to our records, a total of 908 Riverwood employees, past and present, were impacted, with three (3) individuals having addresses in North Dakota.

What happened?

According to information provided by Paperless Pay, on February 18, 2020, an unknown person gained access to their servers where employee data is stored. Paperless Pay discovered the event through notice on February 19, 2020, from the Department of Homeland Security (DHS). In response, Paperless Pay shut down their web server to prevent further access to data. Paperless Pay has been working with the DHS, FBI, and a private forensic security firm to investigate the incident. Ultimately, Paperless Pay was not able to either confirm nor completely rule out the possibility that personal information of our employees was accessed during this incident.

Riverwood noticed the service disruption from Paperless Pay shortly after they shut down their servers and immediately inquired as to the cause of the disruption. Paperless Pay responded that they had a security issue, but did not provide further details in response to Riverwood's questions regarding the nature of the incident, nor did they indicate there was a known data breach at that time. Thereafter Riverwood continued to request more information from Paperless Pay. On March 20, 2020, Paperless Pay provided some additional information, but their communication was ambiguous as to whether personal data of Riverwood employees was actually compromised and, if so, whether it was stored in such a way that the different types of data could be associated to a given, identifiable person. To clarify the facts, we requested a conversation with Paperless Pay, but they did not respond and offer a conversation until April 3, 2020.

During that April 3rd conversation we confirmed that there was no evidence that personal information left the Paperless Pay servers. Nevertheless, Paperless Pay could not rule out the possibility that information they stored might have been obtained by unauthorized individuals, and, if it was, Paperless Pay indicated that individuals with sufficient technical knowledge might be able to associate such information to a specific individual, making it personal information. Paperless Pay also informed us that they had not and did not intend to notify individuals whose data was impacted of this incident and these facts. We were not comfortable with Paperless Pays' decision.

We determined that the right thing for our employees was to send a notice such as this and offer credit monitoring services. We requested a full list of impacted employees from Paperless Pay and received that list on April 23, 2020, and immediately began working with our notice vendor, Kroll, to send this letter and notices to consumers as quickly as possible.

What information was involved?

It is possible that employee information appearing on pay stubs and W2s was compromised. This information may include an individual's name, address, pay and withholdings, and Social Security Number. It is important to note that no protected health information or any other information beyond what is on pay stubs and W2s was impacted by this incident.

What we are doing.

Paperless Pay stated that in addition to the steps mentioned above, they forced password changes, rebuilt their servers, assigned those servers new IP addresses, disabled remote access capabilities, and installed endpoint detection and response to detect intrusions. They have also said that no further compromises to their system have been detected.

Riverwood is evaluating whether to continue the services of Paperless Pay.

For your reference, we are including a copy of the notice letter to consumers that was sent on May 8, 2020. Please contact me if you have further questions.

Sincerely,

Stinson LLP

David Axtell

Riverwood
HEALTHCARE CENTER

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Notice of Data Breach

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We are writing to tell you about a data security incident at our vendor, Paperless Pay, which provides a service that allows our employees to view their pay stubs and W2 forms online. While we do not know that your personal information was obtained by anyone due to this incident, out of an abundance of caution we are providing this notice. We take the safeguarding and proper use of employee information very seriously. For this reason, we are contacting you directly to explain the circumstances of the incident.

What happened?

According to information provided by Paperless Pay, on February 18, 2020, an unknown person gained access to their servers where employee data is stored. Paperless Pay discovered the event through notice on February 19, 2020, from the Department of Homeland Security (DHS). In response, Paperless Pay shut down their web server to prevent further access to data, which you may have noticed shortly after February 19 as an interruption in their service, which then resolved after they instituted further security. Paperless Pay has been working with the DHS, FBI, and a private forensic security firm to investigate the incident. Ultimately, Paperless Pay was not able to either confirm nor completely rule out the possibility that personal information of our employees was accessed during this incident.

We noticed the service disruption from Paperless Pay shortly after they shut down their servers and immediately inquired as to the cause of the disruption. Paperless Pay responded that they had a security issue, but did not provide further details in response to our questions regarding the nature of the incident, nor did they indicate there was a known data breach at that time. Thereafter we continued to request more information from Paperless Pay. On March 20, 2020, Paperless Pay provided some additional information, but their communication was ambiguous as to whether personal data of our employees was actually compromised and, if so, whether it was stored in such a way that the different types of data could be associated to a given, identifiable person. To clarify the facts, we requested a conversation with Paperless Pay, but they did not respond and offer a conversation until April 3, 2020.

During that April 3rd conversation we confirmed that there was no evidence that personal information left the Paperless Pay servers. Nevertheless, Paperless Pay could not rule out the possibility that information they stored might have been obtained by unauthorized individuals, and, if it was, Paperless Pay indicated that individuals with sufficient technical knowledge might be able to associate such information to a specific individual, making it personal information. Paperless Pay also informed us that they had not and did not intend to notify individuals whose data was impacted of this incident and these facts. We were not comfortable with Paperless Pays' decision.

We determined that the right thing for our employees was to send a notice such as this and offer identity monitoring services. We requested a full list of impacted employees from Paperless Pay and received that list on April 23, 2020, and immediately began working to send this letter as quickly as possible.

What information was involved?

It is possible that employee information appearing on your pay stubs and W2s was compromised. This information may include your name, address, pay and withholdings, and Social Security Number. It is important to note that no protected health information or any other information beyond what is on your pay stubs and W2s was impacted by this incident.

What we are doing.

Paperless Pay stated that in addition to the steps mentioned above, they forced password changes, rebuilt their servers, assigned those servers new IP addresses, disabled remote access capabilities, and installed endpoint detection and response to detect intrusions. They have also said that no further compromises to their system have been detected.

We are evaluating whether to continue the services of Paperless Pay.

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services.

*You have until **July 30, 2020** to activate your identity monitoring services.*

Membership Number: `<<Member ID>>`

Additional information describing your services is included with this letter.

What you can do.

Please review the enclosed “Additional Resources” section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

For more information.

If you have questions, please call 1-844-963-2710, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time. Please have your membership number ready.

We recommend using the above listed phone number for any questions and for help with the services we are offering. Safeguarding your information is important to us. We trust that the services we are offering to you demonstrate our continued commitment to your security and satisfaction.

Sincerely,

Casey Johnson
CFO
Riverwood Healthcare

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies is:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual 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's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. 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.

Security Freeze. You have the ability 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 may be able to use an online process, an automated telephone line, or a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, 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.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For New York Residents: You may contact the New York Office of the Attorney General, Bureau of Internet and Technology (BIT), 28 Liberty Street, New York, NY 10005, https://ag.ny.gov/internet/privacy-and-identity-theft; (212) 416-8433.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

For Texas Residents: You are advised that two (2) individuals notified reside in Texas.

To Reach Riverwood Healthcare Center: You may contact Casey Johnson, CFO, 200 Bunker Hill Dr, Aitkin, MN 56431, 1-218-927-5161

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

Kroll | A Division of DUFF & PHELPS

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.