From: Cosentino, Steve <steve.cosentino@stinson.com>
Sent: Friday, September 4, 2020 3:05 PM
To: -Info-Attorney General <ndag@nd.gov>
Subject: Notification of Data Security Incident (North Dakota)

Attorney General Wayne Stenehjem
Office of the Attorney General
600 E Boulevard Ave Dept 125
Bismark, ND 58505

Dear Mr. Stenehjem:

This firm represents Polycystic Kidney Disease Foundation ("PKD Foundation") located in Kansas City, Missouri. We are writing to inform you about a data security incident involving our client, PKD Foundation, that occurred at our client's vendor, Blackbaud, Inc. ("Blackbaud"). Blackbaud is an engagement and fundraising service provider to nonprofits and universities. After thorough investigation and confirmation by Blackbaud we believe that social security numbers, bank account information, or other financial data was not obtained in this data breach. This information was encrypted by Blackbaud. However, certain medical information was potentially accessed by the attacker. Accordingly, the PKD Foundation sent data breach notifications to residents in our state who may have been affected by this incident. According to our records, a total of 741 of North Dakota residents were impacted by this breach.

Description of the Incident

On July 16, 2020, the PKD Foundation was contacted by Blackbaud, one of the world's largest providers of customer relationship management systems for not-for-profit organizations and the higher education sector. Blackbaud representatives informed the PKD Foundation that a Blackbaud service provider had been the victim of a ransomware attack that culminated in May 2020. The cybercriminal was unsuccessful in blocking access to the database involved in the attack, however, the cybercriminal was able to remove a copy of a subset of data from several of Blackbaud's clients including data of Polycystic Kidney Disease Foundation.

What information was involved?

A detailed forensic investigation was undertaken, on behalf of Blackbaud, by law enforcement, and third-party cyber security experts.

As noted above, Blackbaud has confirmed that the investigation found that the cybercriminal did not access credit or debit card information, bank account information or social security number because that information was stored in an encrypted format. Also note that Polycystic Kidney Disease Foundation does not store social security numbers or bank account information.

The Polycystic Kidney Disease Foundation data accessed by the cybercriminal in the Blackbaud database may have contained some of the following information in some of the data records:

- Public information such as name, title, date of birth, spouse;
- Addresses and contact details such as phone numbers and email addresses;
- Philanthropic interests, giving capacity and giving history to the Polycystic Kidney Disease Foundation; and
- Transplant Status.

What is Blackbaud Doing?

The PKD Foundation has been informed by Blackbaud that in order to protect constituent data of Blackbaud clients like Polycystic Kidney Disease Foundation and mitigate potential identity theft, it met the cybercriminal's ransomware demand. Blackbaud advised the PKD Foundation that Blackbaud has received assurances from the cybercriminal and third-party experts that the data was destroyed and thus is no longer usable or accessible by any unauthorized persons or entities. Blackbaud informed the PKD Foundation that Blackbaud continues to monitor the web in an effort to verify the data accessed by the cybercriminal has not been misused.

What is the PKD Foundation doing?

Upon notification of this breach by Blackbaud, the PKD Foundation immediately launched its own investigation and has taken the following steps:

- The PKD Foundation is notifying affected volunteers, donors, employees, chapters, and others in our network that may have been affected to make them aware of this breach of Blackbaud's systems;
- The PKD Foundation is working with Blackbaud to understand why there was a delay between it finding the breach and notifying us, as well as what actions Blackbaud is taking to increase its security to ensure our data will be protected against future threats;
- The PKD Foundation is conferring with other Blackbaud clients to share information about this breach, resulting corrective actions and identify any additional recommended best practices.
- The PKD Foundation is evaluating whether to continue to collect the transplant status field and how to encrypt that field if it continues to be collected.
- Additional notifications regarding this incident will be posted to https://www.pkdcure.org/blackbaud.htm
- PKD Foundation is evaluating whether to continue the services of Blackbaud.

For your reference, we are including a copy of the letter the PKD Foundation is sending. Please contact me if you have further questions.

.

Sincerely,

Steve Cosentino
Partner

STINSON LLP
1201 Walnut Street, Suite 2900
Kansas City, MO 64106-2150
Direct: 816.691.2450 \ Mobile: 913.515.5058 \ Bio

Assistant: Mary Menard \ 816.691.3392 \ mary.menard@stinson.com

STINSON.COM

[DATE]

NOTICE OF DATA BREACH

Dear Member of the PKD Community:

We respect the privacy of your information, which is why, as a precautionary measure, we are writing to let you know about a data security incident that may involve your personal information.

WHAT HAPPENED?

On July 16, 2020, we were contacted by Blackbaud, one of the world's largest providers of customer relationship management systems for not-for-profit organizations and the higher education sector. Company representatives informed us that a Blackbaud service provider had been the victim of a ransomware attack that culminated in May 2020. The cybercriminal was unsuccessful in blocking access to the database involved in the attack, however, the cybercriminal was able to remove a copy of a subset of data from several of Blackbaud's clients including data of Polycystic Kidney Disease Foundation.

WHAT INFORMATION WAS INVOLVED?

We would like to reassure our constituents that a detailed forensic investigation was undertaken, on behalf of Blackbaud, by law enforcement, and third-party cyber security experts. As noted above, Blackbaud has confirmed that the investigation found that the cybercriminal did not access your credit or debit card information, bank account information or social security number because that information was stored in an encrypted format. Also note that Polycystic Kidney Disease Foundation does not store social security numbers or bank account information. The Polycystic Kidney Disease Foundation data accessed by the cybercriminal in the Blackbaud database may have contained some of the following information in some of the data records:

- Public information such as name, title, date of birth, spouse;
- Addresses and contact details such as phone numbers and e-mail addresses;
- Philanthropic interests, giving capacity and giving history to the Polycystic Kidney Disease Foundation; and
- Transplant Status.

WHAT BLACKBAUD IS DOING?

We have been informed by Blackbaud that in order to protect constituent data of Blackbaud clients like Polycystic Kidney Disease Foundation and mitigate potential identity theft, it met the cybercriminal's ransomware demand. Blackbaud has advised us that it has received assurances from the cybercriminal and third-party experts that the data was destroyed and thus is no longer usable or accessible by any unauthorized persons or entities. Blackbaud informs us that it continues

to monitor the web in an effort to verify the data accessed by the cybercriminal has not been misused.

WHAT ARE WE DOING?

Upon notification of this breach by Blackbaud, we immediately launched our own investigation and have taken the following steps:

- We are notifying affected volunteers, donors, employees, and others in our network that may have been affected to make them aware of this breach of Blackbaud's systems;
- We are working with Blackbaud to understand why there was a delay between it finding the breach and notifying us, as well as what actions Blackbaud is taking to increase its security to ensure our data will be protected against future threats;
- We are conferring with other Blackbaud clients to share information about this breach, resulting corrective actions and identify any additional recommended best practices.
- Additional notifications regarding this incident will be posted to www.pkdcure.org/blackbaud.

WHAT YOU CAN DO?

We do not believe there is a need for our constituents to take any action at this time. Although your financial account information was not accessed in this security breach, below is some information about how to protect your financial information should you have other reasons to be concerned. We recommend people remain vigilant and promptly report any suspicious account activity or suspected identity theft to the proper authorities.

- Review Your Account Statements and Notify Law Enforcement of Suspicious Activity.

  As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. 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 also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including your state attorney general and the Federal Trade Commission (FTC).

  To file a complaint with the FTC, go to IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

- Obtain and Monitor Your Credit Report.

  We recommend that you obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an

Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can access the request form at https://www.annualcreditreport.com/requestReport/requestForm.action. Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax
(866) 349-5191
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian
(888) 397-3742
www.experian.com
P.O. Box 4500
Allen, TX 75013

TransUnion
(800) 888-4213
www.transunion.com
2 Baldwin Place
P.O. Box 1000
Chester, PA 19016

- Consider Placing a Fraud Alert on Your Credit Report.

  You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

- Security Freeze.

  In some US states, you have the right to put a security freeze on your credit file. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. It is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to apply for a new credit card, wireless phone, or any service that requires a credit check. You must separately place a security freeze on your credit file with each credit

reporting agency. To place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement, or insurance statement. There is no charge to request a security freeze or to remove a security freeze.

- Take Advantage of Additional Free Resources on Identity Theft.

  We recommend that you review the tips provided by the Federal Trade Commission's Consumer Information website, a valuable resource with some helpful tips on how to protect your information. Additional information is available at https://www.consumer.ftc.gov/topics/privacy-identity-online-security.

  For more information, please visit IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). A copy of Identity Theft – A Recovery Plan, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at https://www.consumer.ftc.gov/articles/pdf-0009_identitytheft_a_recovery_plan.pdf.

FOR MORE INFORMATION

For questions related to the security incident, contact Chad Iseman, Polycystic Kidney Disease Foundation, Chief Advancement Officer, (800) 753-2873, prompt #3 and pkdcure@pkdcure.org.

We will continue to work with Blackbaud to investigate this incident. We regret the inconvenience that this data breach may have caused. Please be assured that we take data protection very seriously and are grateful for the continued support of our alumni and friends.

Sincerely,

[SIGNATURE]

Andy Betts, President and CEO
Polycystic Kidney Disease Foundation