



BRYAN CAVE LEIGHTON PAISNER LLP
1155 F Street NW
Washington DC 20004 1357
T: +1 202 508 6000
F: +1 202 508 6200
www.bcplaw.com

April 8, 2021

Joshua James
Direct: 202/508-6265
Fax: 202/508-6200
josh.james@bcplaw.com

Attorney General Aaron Frey

Office of the Attorney General
SECURITY BREACH NOTIFICATION
Consumer Protection Division
111 Sewall Street, 6th Floor
Augusta, Maine 04330
Fax: 207-624-7730
E-mail: breach.security@maine.gov

VIA EMAIL

Dear Attorney General Frey:

Neighborhood Healthcare, a client of Bryan Cave Leighton Paisner, LLP, is notifying your office that Neighborhood Healthcare is notifying 1 individual who resides in Maine of a data security incident experienced by Neighborhood Healthcare's form hosting service provider, Netgain Technology, LLC ("Netgain").

On November 24, 2020, Netgain became aware of a security incident that involved unauthorized access to portions of the Netgain environment and Netgain client environments and began taking steps to investigate this incident. But, on December 3, 2020, the attacker launched a ransomware attack against Netgain, encrypting a subset of files owned by Netgain and Netgain's clients and disrupting Netgain's operations. In response, Netgain took additional measures to contain the threat and address the issue. Netgain's technical teams worked closely with third-party experts to remove the threat in the impacted environments and confirm that client and internal systems are protected.

Neighborhood Healthcare learned of the ransomware attack on December 3, 2020. At that time, Neighborhood Healthcare had no reason to believe that the protected information of our patients, employees, or vendors had been impacted in the incident. However, on January 7, 2021, Netgain informed Neighborhood Healthcare that some information including, potentially, some files containing patient PHI and vendor/employee personal information may have been impacted in the incident. Netgain could not confirm, at that time, what records may have been impacted in the incident. It was not until January 21, 2021, that Netgain provided a set of files to Neighborhood Healthcare that Netgain believed were impacted by the attackers. Those files came from a Neighborhood Healthcare server accessible by the Netgain environment. Since that time, Neighborhood Healthcare has worked to review those records, to identify individuals impacted, conduct an investigation into the incident with the assistance outside experts, and to transmit letters to impacted individuals with its accompanying protective measures. On March 16, 2021, Neighborhood Healthcare determined what individuals were impacted in the Netgain incident.

Neighborhood Healthcare is mailing notifications to potentially affected individuals in your state on April 8, 2021. An example of the notification is attached. Individuals whose Social Security Number was impacted will receive an offer for identity protection services provided by IDX. Information regarding these services, as well as additional information to assist impacted individuals, is included in the notification sent to the affected individuals.

If you would like additional information concerning the above, please feel free to contact me.

Sincerely,

A handwritten signature in blue ink that reads "Joshua James".

Joshua James



C/O IDX
P.O. Box 989728
West Sacramento, CA 95798-9728

<<FIRST NAME>> <<LAST NAME>>
<<ADDRESS1>>
<<ADDRESS2>>
<<CITY>>, <<STATE>> <<ZIP>>

To Enroll, Please Call:
(833) 903-3642
Or Visit:
<https://response.idx.us/nhc-netgain-incident>
Enrollment Code: <<ENROLLMENT>>

April 8, 2021

Notice of Data Breach

Dear <<FIRST NAME>> <<LAST NAME>>,

The privacy and security of your personal information is very important to Neighborhood Healthcare. We are writing to make you aware of an issue brought to our attention by our former third-party hosting provider, Netgain. Netgain is a leading cloud hosting and managed services provider. Neighborhood Healthcare used Netgain to host some Neighborhood Healthcare files.

What Happened

On November 24, 2020, Netgain became aware of a security incident that involved unauthorized access to portions of the Netgain environment and Netgain client environments and began taking steps to investigate this incident. But, on December 3, 2020, the attacker launched a ransomware attack against Netgain, encrypting a subset of files owned by Netgain and Netgain’s clients and disrupting Netgain’s operations. In response, Netgain took additional measures to contain the threat and address the issue. Netgain’s technical teams worked closely with third-party experts to remove the threat in the impacted environments and confirm that client and internal systems are protected.

Neighborhood Healthcare learned of the ransomware attack on December 3, 2020. At that time, Neighborhood Healthcare had no reason to believe that the protected health information (“PHI”) of our patients had been impacted in the incident. However, on January 7, 2021, Netgain informed Neighborhood Healthcare that some information including, potentially, some files containing patient PHI may have been impacted in the incident. Netgain could not confirm, at that time, what records may have been impacted in the incident. It was not until January 21, 2021, that Netgain provided a set of files to Neighborhood Healthcare that Netgain believed were impacted by the attackers. Those files came from a Neighborhood Healthcare server accessible by the Netgain environment. Since that time, Neighborhood Healthcare has worked to review those records, to identify individuals impacted, conduct an investigation into the incident with the assistance outside experts, and to transmit this letter to you with its accompanying protective measures. On March 16, 2021, Neighborhood Healthcare determined that the impacted files included some of your information.

What Information Was Involved

The information involved may have included some of the following: your name, date of birth, address, Social Security Number and information about the care that you received from Neighborhood Healthcare such as insurance coverage information, physician you saw, and treatment codes. Neighborhood Healthcare is offering credit monitoring services to you at no charge. Please see the **What You Can Do** section below for information about these services including how to enroll. Please also see the **Additional Important Information** section below for further precautionary measures you may wish to take. Netgain has received assurances that the data has not gone beyond the attacker, that the data was not and will not be misused, and that the data will not be disseminated or otherwise be made publicly available.

What We Are Doing

Please know that we take this incident and the security of your personal information very seriously. Ensuring the safety of our patients' data is of the utmost importance to us. Since we learned of this incident, we have been working with Netgain to seek assurances that they are taking appropriate steps to respond to this incident. We have also conducted an investigation of the incident with the help of outside experts, and we have transitioned to a new hosting provider (a transition that was already in process when this incident occurred).

In addition, we are providing you with steps that you can take to help protect your personal information, and as an added precaution, we are offering you complimentary identity protection services through IDX, a leader in risk mitigation and response. These services include <<12/24 months>> of credit monitoring, dark web monitoring, a \$1,000,000 identity fraud loss reimbursement policy, and fully-managed identity theft recovery services.

What Netgain Is Doing

Netgain took several steps to strengthen its environment following the incident, including international Geo-fencing for Azure-hosted environments, deploying additional log monitoring across all servers, and additional hardening of network security rules and protocols to restrict lateral movement across environments. Netgain stated that it paid a significant amount to the attacker in exchange for assurances that the attacker will delete all copies of this data and that it will not publish, sell, or otherwise disclose the data. In addition, Netgain's cybersecurity experts conducted regular dark web scans for the impacted files, but such searches have not yielded any indications that the data involved in this incident has been or will be published, sold, offered for sale, or otherwise disclosed. Accordingly, there is no reason to believe that any information involved in the incident has been or will be misused.

What You Can Do

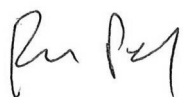
We recommend that you review the additional information enclosed. Additionally, we encourage you to contact IDX with any questions and to enroll in free identity protection services by calling (833) 903-3642 or going to <https://response.idx.us/nhc-netgain-incident> and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is July 8, 2021.

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. IDX 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

We very much regret any inconvenience this incident may cause you. Should you have any further questions or concerns regarding this matter, please call (833) 903-3642, Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time.

Sincerely



Rakesh Patel
CEO
Neighborhood Healthcare

Additional Important Information

1. Website and Enrollment. Go to <https://response.idx.us/nhc-netgain-incident> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at (833) 903-3642 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Generally. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing financial account statements and monitoring your credit reports for unauthorized activity. 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. You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to your state's Attorney General.

5. The FTC. You can obtain information from Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft

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

6. Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf), Experian (<https://www.experian.com/fraud/center.html>), or Transunion (<https://www.transunion.com/fraud-victim-resource/place-fraud-alert>). 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. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

7. 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, 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; (5) Proof of current address, such as current utility or telephone bill, bank or insurance statement; (6) legible photocopy of 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. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. It is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348-5788 equifax.com/personal/credit-report-services/ 800-525-6285	Experian Security Freeze P.O. Box 9554 Allen, TX 75013-9544 experian.com/freeze/center.html 888-397-3742	TransUnion (FVAD) P.O. Box 160 Woodlyn, PA 19094 transunion.com/credit-freeze 888-909-8872
---	--	---

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

8. Protecting Medical Information: To date, we have no reason to believe that your PHI potentially involved in this incident was or will be used for any unintended purposes. As a general matter, however, the following steps can help protect you from medical identity theft issues.

- Do not share health insurance cards with anyone apart from your care providers and other family members who are covered under the insurance plan or who help you with your medical care.
- Review the “explanation of benefits statements” that you receive from your health insurance company. If you see something amiss, follow up with your insurance company or the health care provider identified on the explanation of benefits to request further information.
- Ask your health insurance company for a report on all services they have paid for you for the current year. If you do not recognize an item in that list, speak with your insurance company to verify it.

9. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201904_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.