

Dianne K. Pledge dpledgie@ftlf.com

January 7, 2022

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

To Whom It May Concern,

We represent the National Association of Community Health Centers (NACHC), located at 7501 Wisconsin Ave, Suite 1100W, Bethesda, MD 20814, and are writing to notify your office of a recent security incident that may affect the security of some personal information of residents of Maryland. Below please find additional details about the security incident and NACHC's response.

Brief Description of the Nature of the Security Breach

On October 5, 2021, after receiving reports from users of system slowness and other issues, NACHC discovered that one of its servers had been compromised by a cyberattack. NACHC immediately took the server offline and launched an internal investigation that included running malware and antivirus scans, restricting access, restoring and updating the systems, requiring users to change their passwords and notifying users about the incident. The compromised server did not contain personal information.

On October 16, 2021, NACHC discovered that another of its servers had been compromised by a cyberattack. NACHC immediately took the server offline and engaged an outside cybersecurity firm to conduct a comprehensive investigation to confirm the full nature and scope of the security incidents. The investigation, completed on December 13, 2021, confirmed the threat actors initially gained access on or around October 4, 2021. They then accessed multiple servers, including one that stored personal information of current and past employees and contractors. The investigation was unable to determine whether any personal information was exfiltrated as part of the cyberattacks.

Number of Maryland Residents Being Notified

On December 27, 2021, NACHC confirmed that the personal information of 202 Maryland residents was stored on the compromised servers. On January 10, 2022, NACHC will provide written notice of this incident. Attached is a sample of the notification. It includes a description of the breach, details about the personal information involved and instructions on how to access 24 months of free credit monitoring and identity theft recovery services.

Information Compromised

For current and past employees, the personal information included names, addresses, Social Security numbers, salary information and date of birth. For current and past contractors, the personal information included names, addresses and Social Security numbers. At this time, there is no evidence that this information has been misused.

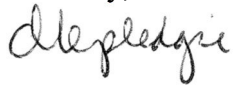
Steps NACHC is Taking to Restore Integrity of the System

NACHC improved the security of its systems to protect against future cyberattacks by moving systems to third-party hosted environments (when possible), implementing two-factor authentication, and contracting with a cybersecurity firm to implement preventive measures, such as monitoring, testing and auditing of our systems on an individual and network level.

Contact Information

Should you have any questions regarding this notification or other aspects of the security incidents, please contact me at dpledgie@ftlf.com or 202-466-8960.

Sincerely,

A handwritten signature in black ink, appearing to read "Dpledgie", written in a cursive style.

Dianne K. Pledgie, Esq.

Attachment: Notification – Employees - FINAL



<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

To Enroll, Please Call:
1-800-939-4170
Or Visit:
<https://app.idx.us/account-creation/protect>
Enrollment Code: <<XXXXXXXXXX>>

January 10, 2022

Notice of Data Breach

Dear <<First Name>> <<Last Name>>,

I am writing to inform you about a recent security incident that may impact your personal information. While there is no evidence that your personal information has been misused, the National Association of Community Health Centers (NACHC) is providing this notice, recommending steps to protect your identity and offering free identity protection services.

What Happened

On October 16, 2021, NACHC discovered that certain systems, including a database that stored information on past and current employees, were inaccessible. After an initial internal investigation, NACHC engaged an outside cybersecurity firm to conduct a comprehensive investigation to confirm the full nature and scope of the security incident. The investigation, completed on December 13, 2021, determined that threat actors accessed and encrypted several servers as part of a coordinated cyberattack. The investigation was unable to determine whether data on the compromised servers was exfiltrated. Because your personal information was stored on the compromised servers, NACHC is providing this notice.

What Information Was Involved

The information included employee names; addresses; dates of birth; salary, income and tax information; Social Security numbers; type of insurance coverage along with beneficiary names; emergency contact names; and employee start dates.

What We Are Doing

NACHC reported the cyberattack to law enforcement (including the FBI, Department of Homeland Security, the Department of Treasury and the local police) and is improving the security of its systems to protect against future cyberattacks. In addition, NACHC is offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include 24 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do

The events that occurred do not automatically mean that you are a victim of identity theft. We encourage you to remain vigilant; to continually review your credit report, bank account activity, and bank statements for irregularities or unauthorized items; and to immediately report any unauthorized accounts or charges to your financial institution.

We also encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-800-939-4170 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 6 am - 6 pm Pacific Time. Please note the deadline to enroll is April 10, 2022.

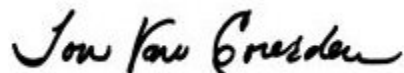
Again, at this time, there is no evidence that your information has been misused; however, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal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

For More Information

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 1-800-939-4170 or go to <https://app.idx.us/account-creation/protect> for assistance or for any additional questions you may have.

Sincerely,

A handwritten signature in black ink that reads "Tom Van Coverden". The signature is written in a cursive, flowing style.

Tom Van Coverden
NACHC President and CEO

(Enclosure)



Recommended Steps to Help Protect Your Information

- 1. Website and enrollment.** Go to <https://app.idx.us/account-creation/protect> 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 1-800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.
- 4. Review your credit reports.** We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

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 the Attorney General.

5. Place fraud alerts. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert 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. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Place a security freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. 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.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

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/201504_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. Three Rhode Island residents were impacted by this security incident.

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.