WILSON ELSER
WILSON ELSER MOSKOWITZ EDELMAN & DICKER LLP

December 9, 2021

RECEIVED
DEC 14 2021
CONSUMER PROTECTION

Ross M. Molina, Esq.
504.702.1726 (direct)
Ross.Molina@WilsonElser.com

VIA U.S. MAIL:

Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03302

Re:	**Our Client**	**:**	**San Ysidro Health**
	Matter	**:**	**Netgain Data Security Incident on May 24, 2020**
	Wilson Elser File #	**:**	**16516.01003**

Dear Attorney General McDonald:

We represent San Ysidro Health ("SYH"), which is based in San Diego, California. Our representation of SYH relates to a potential data security incident involving its third-party cloud hosting vendor, Netgain, described in more detail below. SYH takes the security and privacy of the information in its control seriously, and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve to inform you of the nature of the security incident, the number of New Hampshire residents being notified (9), what information has been impacted, and the steps that SYH is taking to restore the integrity of the system. We have also enclosed hereto a sample of the notification made to the potentially impacted individual(s), which includes an offer of free credit monitoring.

1. Nature of the Security Incident

On December 4, 2020, Netgain notified all of its customers that it had experienced a cybersecurity incident. SYH, along with thousands of other businesses, retained Netgain for online hosting of its environment, including cloud services and e-mail. The cybersecurity incident blocked SYH's access to its Netgain-hosted environment for approximately three weeks.

Upon notification of the incident, SYH worked with its information technology (IT) support team and engaged a law firm specializing in cybersecurity and data privacy to investigate further. It also stayed in close communication with Netgain and its breach counsel regarding Netgain's incident response and forensic investigation.

On January 15, 2021, Netgain notified SYH that some of the data hosted by Netgain may have been removed from the network during the cybersecurity incident. SYH then immediately moved forward with an extensive data mining project to identify the individuals whose sensitive information were potentially impacted. SYH provided data breach notifications to potentially

impacted individuals in phases as the individuals were identified. Based on the results of the most recent portion of the data mining investigation, which concluded on December 1, 2021, SYH has determined that additional individuals' certain information - including name, social security number, medical treatment history, and other personal information - were potentially accessed by an unknown party that is not authorized to handle or view such information. **At this time, SYH does not have any evidence to indicate that any personal information has been or will be misused as a result of this incident. Further, SYH has not received any reports of related identity theft since the date of the incident.**

2. Number of New Hampshire Residents Affected

A total of 9 residents of New Hampshire were potentially affected by this security incident. A notification letter to this individual was mailed on December 9, 2021, by first class mail. A sample copy of the notification letter is included with this letter.

3. Steps Taken

In light of this incident, SYH has replaced Netgain as its hosting vendor and is migrating its environment and data to another service provider that has assured SYH that the data will be hosted in such a way that it cannot be exposed in a similar attack. Additionally, SYH is conducting an investigation with the assistance of third-party forensic specialists and confirming the security of its network environment. Further, SYH has offered free credit monitoring services to all potentially affected individuals.

4. Contact Information

SYH remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Ross.Molina@WilsonElser.com or 504.702.1726.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Ross M. Molina

Copy: Robert Walker, Esq. (Wilson Elser LLP)

Enclosure: *Sample Notification Letter*

SAN YSIDRO HEALTH

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

To Enroll, Please Call:
1-833-820-0975
Or Visit:
https://response.idx.us/syh
Enrollment Code:<<Enrollment>>

Via First-Class Mail

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

December 9, 2021

Notice of Data Breach

Dear <<First Name>> <<Last Name>> <<Suffix>>:

Centro De Salud De La Comunidad De San Ysidro ("SYH") is a non-profit health care facility with 42 program sites across San Diego County, California. We recently discovered that a data security incident on Netgain's environment may have resulted in the unintentional exposure of your personal information. This letter contains additional information about the incident, our response to this incident, and steps you can take to protect yourself. Please be assured that SYH takes the protection and proper use of personal information very seriously, and we sincerely apologize for any inconvenience this may cause.

What Happened

Netgain is a third-party entity that offers hosting and cloud IT solutions primarily for the healthcare and accounting industry. SYH, along with thousands of other healthcare entities, retained Netgain for online hosting of its environment, including cloud services and e-mail. Netgain was recently the target of a cybersecurity incident. Upon discovery, we worked with our information technology (IT) support team and engaged a law firm specializing in cybersecurity and data privacy to investigate further. We have also stayed in close communication with Netgain and its breach counsel regarding Netgain's incident response and forensic investigation. Based on the results of this investigation to date, we have determined that information, including your name, <<Variable1>>, were accessed by an unknown party that is not authorized to handle or view such information. **At this time, SYH does not have any evidence to indicate that any of your personal information has been or will be misused as a result of this incident. Nevertheless, SYH decided to notify you of this incident out of an abundance of caution.**

What We Are Doing

In light of this incident, SYH is actively assessing ways we can further improve our cybersecurity posture. As a safeguard, we have arranged for you to enroll in a complementary, online credit monitoring service for <<12/24>> provided by IDX. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do:

We recommend you take advantage of the following resources:

- **Contact IDX for questions and support** - We encourage you to contact IDX with any questions and to **enroll in free IDX services** by calling 1-833-820-0975 or by going to https://response.idx.us/syh and using the Enrollment Code provided above. IDX is available Monday through Friday 6 am – 6 pm Pacific Time. Please note the deadline to enroll is March 9, 2022.
- **Credit Report** - Obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account.

- **Security Freezes** - You 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.
- **Fraud Alerts** - Fraud alerts tell creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts.
- **Monitoring** - Remain vigilant and monitor your accounts for suspicious or unusual activity.

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

Please know that the protection of your personal information is a top priority, and we sincerely regret any concern or inconvenience that this matter may cause you. If you have any questions, please do not hesitate to call IDX for questions and support at 1-833-820-0975, Monday through Friday 6 am – 6 pm Pacific Time.

Sincerely,

Kevin Mattson
President and CEO

Additional Information

Credit Reports: 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.

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; 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 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	**Experian Security Freeze**	**TransUnion Security Freeze**
P.O. Box 105788 Atlanta, GA 30348 1-800-349-9960 https://www.equifax.com/personal/credit-report-services/credit-freeze/	P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	P.O. Box 160 Woodlyn, PA 19094 1-800-909-8872 www.transunion.com/credit-freeze

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);
- TransUnion (https://www.transunion.com/fraud-alerts); or
- Experian (https://www.experian.com/fraud/center.html).

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 phone numbers for all three credit bureaus are at the bottom of this page.

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

File Police Report: You have the right to file or obtain a police report if you 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 proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

FTC and Attorneys General: You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law

enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, and www.oag.state.md.us.

For 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 violators. 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. We encourage you to review your rights pursuant to the Fair Credit Reporting Act at 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.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, and www.ncdoj.gov.

For 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, and https://ag.ny.gov/.

For Rhode Island residents, the Rhode Island Attorney General can be reached at 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.