

# STUDEBAKER | NAULT

BARBRA Z. NAULT, ESQ.  
*Admitted in Washington, Oregon and Alaska*  
11900 N.E. 1st Street, Suite 300  
Bellevue, WA 98005  
bnault@studebakernault.com

February 17, 2021

VIA E-Mail

Office of the Attorney General  
1125 Washington Street SE  
P.O. Box 40100  
Olympia, WA 98504-0100  
E-Mail: [SecurityBreach@atg.wa.gov](mailto:SecurityBreach@atg.wa.gov)

Dear Attorney General Ferguson:

This letter is to inform your office of a recent data security incident involving personal information of Washington residents maintained by Woodcreek Provider Services, LLC. This letter describes the incident, what the incident investigation has revealed so far about the information involved and potentially affected individuals, and the steps Woodcreek Provider Services has taken in response to the incident.

## **Background**

Woodcreek Provider Services, LLC provides medical practice management and support to several pediatric clinics and urgent care centers owned and operated by MultiCare Health System, including certain clinics that were previously owned and operated by Woodcreek Healthcare. Woodcreek Provider Services contracts with Netgain Technology, LLC (“Netgain”) to host its information technology network and computer systems.

## **Nature of the Data Event**

On January 4, 2021, Woodcreek Provider Services was notified that Netgain’s systems had been compromised, but the impact on Woodcreek Provider Services data was unknown. Additional details about the incident were provided on January 14, 2021. At that time, Netgain reported a security incident that involved unauthorized access to portions of the Netgain environment which Netgain had discovered in late November 2020 but may have occurred as early as September 2020. According to Netgain, it took prompt action to deploy its incident response plan and investigate the incident, engaged leading third-party cybersecurity experts, notified law enforcement, and rolled out additional security enhancements within its network.

According to Netgain, on December 3, 2020, the criminal attackers launched a ransomware attack, encrypting a subset of Netgain's clients and internal systems. In response, Netgain reported it took measures to contain the threat, including disabling external and internal network pathways and taking client services offline. Netgain reported that its investigation indicated data was exfiltrated from Woodcreek Provider Services' hosted environment prior to the ransomware deployment on December 3, 2020. Netgain reported that it paid the threat attackers and recovered Woodcreek Provider Services' information. According to Netgain, it received assurances that the attackers deleted the data and did not retain any copies. Netgain reported that through law enforcement channels and its cybersecurity expert's engagements with this threat actor, Netgain was informed that once payment is made, the threat actors are not known to post the data nor keep any copies of it. As an added precaution, Netgain reported its cybersecurity experts continue to monitor for any signs that the data exfiltrated has been posted for sale, and that as of January 14, 2021, no such indications have been identified.

According to Netgain, it installed additional advanced threat protection and monitoring software (SentinelOne) across its systems to proactively safeguard against future threats and conducted thorough scans of its environment to identify potential impacts from this attack. Netgain reported it is working to promptly address any new vulnerabilities that may be identified. According to Netgain, the threat to its environment had been contained and eradicated as of January 14, 2021.

On January 18, 2021, Woodcreek Provider Services received a copy of the data set recovered by Netgain and immediately began the process of reviewing the data to identify the information involved and the individuals potentially affected by the incident. The recovered data set included approximately 215,000 directories and 21,874 file folders. Woodcreek Provider Services' review determined that the recovered data set includes "personal information" as that term is defined by RCW 19.255.005, as well as protected health information as that term is defined under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

The recovered data set includes the following types of personal information from business records maintained by Woodcreek Provider Services: full names, dates of birth, social security numbers, student identification numbers, health insurance policy numbers, bank account numbers (from direct deposit forms and voided checks), resumes, transcripts, performance appraisals, criminal background check reports, court documents related to garnishments, court orders and decrees, copies of diplomas, degrees, board certifications, Drug Enforcement Agency certificates, payroll withholding authorizations for 401k elections and insurance deduction authorizations, benefit enrollment forms, payroll tax forms (W2s, W4s, 1095s, & K1s), and employee health information, including vaccination records, on-the-job injury reports and safety incident reports.

The recovered data set also includes protected health information maintained by Woodcreek Provider Services, Woodcreek Healthcare and/or MultiCare Health System, including patient names and addresses, medical record numbers, dates of birth, insurance identification numbers, insurance claims information, explanation of benefits, statements, clinical notes, referral requests, laboratory reports, decision not to vaccinate forms, authorization requests for services, treatment approvals, records requests, immunization information, vaccine records, prescription

requests, release of information forms, subpoena records requests, medical record disclosure logs, incident reports, invoices, correspondence with patients, and some medical records. The primary electronic medical records database was not affected by this incident.

### **Notice to Washington Residents**

Woodcreek Provider Services engaged ID Experts to assist with providing notification of this incident to affected Washington residents and others.

Woodcreek Provider Services initially identified 557 employees, healthcare providers, applicants, and contractors whose personal information was in the recovered data set. Written notification in the form attached hereto is being mailed to those individuals with verified contact information on February 17, 2021.

An additional group of 25,360 individuals entitled to notice were subsequently identified within the recovered data set because their personal information was associated with individuals receiving services delivered by either Multicare Health System or Woodcreek Healthcare. Written notification in the form attached hereto is being prepared and will be mailed to those individuals with verified contact information on or about February 26, 2021.

The written notification being mailed to these individuals includes an offer to enroll in free credit monitoring and identity theft protection services provided by ID Experts and paid for by Woodcreek Provider Services. The notification also provides a phone number to a call center (1-833-726-0944) and website (<https://response.idx.us/woodcreek>) with information for individuals who have questions about the incident or the enrollment process.

Woodcreek Provider Services has also engaged Mackenzie Marketing to distribute media notification of the incident and will be posting information and a link to the ID Experts website on the Woodcreek Provider Services website.

### **Other Steps Taken and To Be Taken**

Woodcreek Provider Services is in regular communication with Netgain to ensure they are taking appropriate steps to better maintain the security of Woodcreek Provider Services' and MultiCare Health System's hosted data.

Woodcreek Provider Services is a business associate of MultiCare Health System as that relationship is defined in HIPAA and is also complying with the requirements of HIPAA in responding to this incident. An additional group of approximately 210,000 individuals will receive notification of this incident as required by HIPAA.

Woodcreek Provider Services has also provided the Drug Enforcement Agency with a list of provider numbers that were potentially affected by this incident and is encouraging providers to contact the Drug Enforcement Agency for a new provider number.

Although Woodcreek Provider Services was not targeted in the attack, the company is taking steps to enhance its cybersecurity protocols and practices, including reminding all staff to regularly change passwords, conducting a thorough review of stored information, and updating its data retention policies.

Office of the Attorney General

February 17, 2021

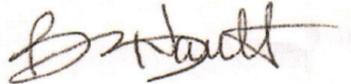
Page 4

**Contact Information**

If there are questions about the information in this letter, please contact the undersigned or James Hudson, CEO, Woodcreek Provider Services LLC, at [jhudson@woodcreekhealthcare.com](mailto:jhudson@woodcreekhealthcare.com) or 253-446-3204.

Regards,

STUDEBAKER NAULT, PLLC

A handwritten signature in black ink, appearing to read "B. Nault", is written over a light grey rectangular background.

Barbra Z. Nault

Enclosure: 2021-02-10 DRAFT Individual Notice WA\_v2 (PRINT PROOF)



C/O IDX  
10300 SW Greenburg Rd., Suite 570  
Portland, OR 97223

To Enroll, Please Call:  
1-833-726-0944  
Or Visit:  
<https://response.idx.us/woodcreek>  
Enrollment Code: <<XXXXXXXXXXXX>>

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

February 17, 2021

### Notice of Data Breach

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

#### What Happened

We are writing to inform you of a security breach that may have involved your personal information.

Our company, Woodcreek Provider Services, LLC, provides medical practice management and support to several pediatric clinics and urgent care centers owned and operated by MultiCare Health System, some of which were previously owned and operated by Woodcreek Healthcare. We contract with Netgain Technology, LLC, to host our information technology network and computer systems. On January 4, 2021, we were notified by Netgain Technology that its systems had been compromised by a cyberattack in the fall of 2020. After discovering the cyberattack, Netgain Technology notified law enforcement and paid ransom to regain control of its systems and recover the affected data. On January 18, 2021, Netgain Technology identified the Woodcreek Provider Services, MultiCare Health System and Woodcreek Healthcare data involved in the cyberattack. We immediately began the process of reviewing the data to identify the information involved and the individuals potentially affected by this incident.

#### What Information Was Involved

The data that was involved in the cyberattack on Netgain Technology's systems included the following types of personal information from business records maintained by Woodcreek Provider Services: full names, dates of birth, social security numbers, student identification numbers, health insurance policy numbers, bank account numbers (from direct deposit forms and voided checks), resumes, transcripts, performance appraisals, criminal background check reports, court documents related to garnishments, court orders and decrees, copies of diplomas, degrees, board certifications, Drug Enforcement Agency certificates, payroll withholding authorizations for 401k elections and insurance deduction authorizations, benefit enrollment forms, payroll tax forms (W2s, W4s, 1095s, & K1s), and employee health information, including vaccination records, on-the-job injury reports and safety incident reports. Affected individuals include employees, healthcare providers, applicants, contractors and individuals receiving services delivered by either Multicare Health System or Woodcreek Healthcare.

#### What We Are Doing

We are communicating regularly with Netgain Technology to ensure they are taking appropriate steps to better maintain the security of Woodcreek Provider Services data.

Netgain Technology has provided written assurances that the threat to its systems has been contained and eradicated. Netgain Technology reports that it is continuing to scan its environment to identify potential impacts from the attack and will work promptly to address any new vulnerabilities that may be identified. Netgain Technology reports that it has added security

enhancements within its network, including the installation of additional advanced threat protection and monitoring software (SentinelOne) across its systems to proactively safeguard against future threats. Netgain Technology reports it has taken additional steps to prevent similar incidents in the future, including: blocking identified malicious IP addresses, enabling international Geo-fencing for Azure-hosted environments, performing additional hardening of network security protocols surrounding its support environment, reviewing and restricting access rights for all privileged accounts, deploying additional log monitoring across all servers, auditing and strengthening of its access management policies, performing additional hardening of network security rules and protocols to restrict lateral movement across environments, and resetting passwords.

Although Woodcreek Provider Services was not targeted in this cyberattack, we are taking steps to enhance our own cybersecurity protocols and practices, including reminding all staff to regularly change passwords, conducting a thorough review of information stored on our network, and updating our data retention policies. Additionally, Woodcreek Provider Services has provided the Drug Enforcement Agency with a list of provider numbers that were potentially affected by this incident and encouraging providers to contact the Drug Enforcement Agency for a new provider number.

It is our understanding that all the ransomed data was recovered by Netgain Technology and we are not aware that any data was further disclosed or used by those responsible for the cyberattack. However, out of an abundance of caution, we are offering identity theft protection services through IDX, the data breach and recovery services expert.

IDX identity protection services include: 12 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**

We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-833-726-0944 or going to <https://response.idx.us/woodcreek> 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 May 17, 2021.

We recommend that you regularly review the explanation of benefits provided by your health care insurer, credit card statements, and bank accounts for suspicious activity. Any unusual service or charge should be reported to the appropriate financial institution, insurer or health care program immediately. If you suspect that someone is using your personal information to obtain medical services or incur charges without your permission, please report this to the local police department immediately.

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 1-833-726-0944 or go to <https://response.idx.us/woodcreek> for assistance or for any additional questions you may have.

Sincerely,



James Hudson, CEO  
Woodcreek Provider Services

(Enclosure)



## Recommended Steps to Help Protect Your Information

- 1. Website and Enrollment.** Go to <https://response.idx.us/woodcreek> 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 1-833-726-0944 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](http://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** with the three credit bureaus. 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](http://www.equifax.com)

Experian Fraud Reporting  
1-888-397-3742  
P.O. Box 9554  
Allen, TX 75013  
[www.experian.com](http://www.experian.com)

TransUnion Fraud Reporting  
1-800-680-7289  
P.O. Box 2000  
Chester, PA 19022-2000  
[www.transunion.com](http://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. 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](http://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](http://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](http://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](http://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](http://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/](http://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](http://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](http://www.consumer.gov/idtheft), 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.