VedderPrice

Chicago
New York
Washington, DC
London
San Francisco
Los Angeles
Singapore
vedderprice.com

Blaine C. Kimrey
Shareholder
+1 312 609 7865
bkimrey@vedderprice.com

September 12, 2019

VIA E-MAIL (SecurityBreach@atg.wa.gov)
Washington Office of the Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100

Re: Notice of Data Security Incident

Dear Sir or Madam:

I represent Peoples Injury Network Northwest ("PINN"). I'm writing to inform you of a recent data security incident at PINN that may have impacted the security of certain personal information of approximately 12,502 Washington residents.

Background of the Incident

PINN is a physical rehabilitation company focused on industrial rehabilitation patients headquartered in Kent, Washington, with a total of seven locations throughout Washington. On August 8, 2019, PINN discovered that certain personal information of patients and former patients with addresses in Washington could potentially be at risk.

On April 22, 2019, three PINN servers were infected with ransomware, which was discovered on April 23, 2019. PINN immediately took those servers offline and was able to restore most of the data from back-ups. To ensure that PINN's systems were secure and determine if any data was compromised, PINN retained a computer forensics firm to analyze the servers. That firm ***did not find any evidence that personal information was accessed or exfiltrated by the attacker***, but it also could not rule out the possibility of access or exfiltration. Because the servers at issue contained personal information for PINN patients through April 22, 2019, PINN is erring on the side of caution and concluding that all such information could be at risk.

The information at issue included a broad range of personal information and protected health information, including diagnosis information, names, addresses, dates of birth, and driver's license numbers.

Notice to Washington Residents

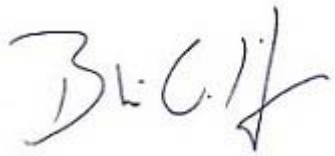
On September 12, 2019, the 12,502 Washington residents for whom PINN had addresses were notified of the incident via direct notice, and substitute notice was provided as well. Enclosed

please find (1) a copy of the letter sent to patients with addresses on file, (2) a copy of the notice that will be posted on PINN's Web site, and (3) a copy of the press release that will be sent to the *Seattle Times*. PINN has arranged to provide one (1) year of complimentary credit monitoring and identity theft protection services through ID Experts for the affected residents. Additionally, PINN has established a call center that the affected residents can contact, toll-free, to ask questions and to receive further information regarding the incident.

Contact Information

Please contact me if you have any questions or if I can provide you with any further information concerning this matter. Thank you.

Sincerely,



Blaine C. Kimrey

cc: PINN

PEOPLES INJURY NETWORK NORTHWEST

C/O ID Experts
PO Box 4219
Everett WA 98204

ENDORSE

NAME
ADDRESS1
ADDRESS2
CSZ

BREAK

SEQ
CODE 2D

To Enroll, Please Call:
833-959-1348
Or Visit:
https://ide.myidcare.com/pinn
Enrollment Code:
<<XXXXXXXX>>

September 12, 2019

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

Peoples Injury Network Northwest ("PINN") values your trust and confidence in us, and we're committed to securing our information systems and your personal information and protected health information ("PHI"). Accordingly, we're writing to make you aware of an incident that may have affected you.

What Happened

On August 8, 2019, PINN discovered that your personal information and PHI could potentially be at risk. On April 22, 2019, three PINN servers were infected with ransomware, which was discovered on April 23, 2019. PINN immediately took those servers offline and was able to restore most of the data from back-ups. To ensure that PINN's systems were secure and determine if any data was compromised, PINN retained a computer forensics firm to analyze the servers. That firm did not find any evidence that personal information was accessed or exfiltrated by the attacker, but it also could not rule out the possibility of access or exfiltration. Because the servers at issue contained personal information for PINN patients through April 22, 2019, PINN is erring on the side of caution and concluding that all such information could be at risk. Accordingly, we're providing this notice to you.

What Information Was Involved

The information at issue could include your name, address, date of birth, driver's license number, and diagnosis information.

What We Are Doing

Investigation. Upon learning about the incident, PINN immediately took the infected servers offline and retained a computer forensics vendor to confirm the scope of the issue.

Mitigation. PINN has retained ID Experts® to provide, at no cost to you, identity theft protection and credit monitoring services. The details for opting in to these services are set forth below.

Protection Against Further Harm. The attacker's access to PINN's systems has been terminated and the infected servers have been taken off line. PINN is not aware of any ongoing threat to its network environment.

What You Can Do

We're offering identity theft protection services through ID Experts®, the data security incident and recovery services expert, to provide you with MyIDCare™. With this protection, MyIDCare will help you resolve issues if your identity is compromised. We strongly encourage you to register for this free identity theft protection service. To enroll please visit https://ide.myidcare.com/pinn or call 833-959-1348 with the Enrollment Code provided above. The deadline for enrollment is December 12, 2019.

Your 12-month MyIDCare membership will include the following:

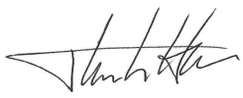
Credit Monitoring and Recovery Services

- **Single-Bureau Credit Monitoring -** Monitors any changes reported by Experian to your credit report.
- **CyberScan** - Dark Web monitoring of underground websites, chat rooms, and malware, 24/7, to identify trading or selling of personal information like SSNs, bank accounts, email addresses, medical ID numbers, driver's license numbers, passport numbers, credit and debit cards, phone numbers, and other unique identifiers.
- **Access to the ID Experts Team** - Access to an online resource center for up-to-date information on new identity theft scams, tips for protection, legislative updates and other topics associated with maintaining the health of your identity.
- **Complete Recovery Services** - Should you believe that you are a victim of identity theft, MyIDCare will work with you to assess, stop, and reverse identity theft issues.
- **Identity Theft Insurance** - In the event of a confirmed identity theft, you may be eligible for reimbursement of up to $1,000,000 for expenses related to that theft.

For More Information

If you have questions or concerns, please contact our toll free number, 833-959-1348, between the hours of 6 am – 6 pm PST. Additionally, for more information about avoiding identity theft, you can contact the Federal Trade Commission at 600 Pennsylvania Ave. N.W., Washington, D.C. 20580, 1-877-ID-THEFT, consumer.ftc.gov.

Sincerely,



Tom Hall
CEO
Peoples Injury Network Northwest

MyIDCare™

Recommended Steps to Help Protect Your Information

1. **Website and Enrollment.** Go to https://ide.myidcare.com/pinn 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 MyIDCare 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, MyIDCare will be able to assist you.

3. Telephone. Contact MyIDCare at 833-959-1348 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 MyIDCare, notify them immediately by calling or by logging into the MyIDCare 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	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.alerts.equifax.com	www.experian.com	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.

SEQ
CODE 2D

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 (http://www.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.

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 U.S. 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.

Notice of Data Security Incident

Peoples Injury Network Northwest ("PINN") values your trust and confidence in us, and we are committed to securing our information systems and your personal information and protected health information ("PHI"). Accordingly, we're issuing this notice of an incident that could affect PINN patients.

What Happened

On August 8, 2019, PINN confirmed that certain personal information and PHI of patients and former patients could potentially be at risk. On April 22, 2019, three PINN servers were infected with ransomware, which was discovered on April 23, 2019. PINN immediately took those servers offline and was able to restore most of the data from back-ups. To ensure that PINN's systems were secure and determine if any data was compromised, PINN retained a computer forensics firm to analyze the servers. That firm did not find any evidence that personal information was accessed or exfiltrated by the attacker, but it also could not rule out the possibility of access or exfiltration. Because the servers at issue contained personal information for PINN patients through April 22, 2019, PINN is erring on the side of caution and concluding that all such information could be at risk.

What Information Was Involved

The information at issue could include the names, addresses, dates of birth, driver's license numbers, and diagnosis information for patients and former patients.

What We Are Doing

Investigation. Upon learning about the incident, PINN immediately took the infected servers offline and retained a computer forensics vendor to confirm the scope of the issue.

Mitigation. PINN has retained ID Experts to provide, at no cost to you, credit monitoring and identity theft protection services and insurance. To take advantage of these services, PINN patients should call 833-959-1348.

Protection Against Further Harm. The attacker's access to PINN's systems has been terminated and the infected servers have been taken off line. PINN is not aware of any ongoing threat to its network environment.

For More Information

If you have questions or concerns, please contact ID Experts at 833-959-1348 between the hours of 6 am – 6 pm PST. Additionally, for more information about avoiding identity theft, you can contact the Federal Trade Commission at 600 Pennsylvania Ave. N.W., Washington, D.C. 20580, 1-877-ID-THEFT, consumer.ftc.gov.

FOR IMMEDIATE RELEASE

Kent, Wash. -- Peoples Injury Network Northwest ("PINN"), a physical rehabilitation company with a total of seven locations throughout Washington, is providing notice of a data security incident that could have affected anyone who was a patient of PINN's before April 22, 2019.

On August 8, 2019, PINN confirmed that certain personal information and protected health information ("PHI") of patients and former patients could potentially be at risk. On April 22, 2019, three PINN servers were infected with ransomware, which was discovered on April 23, 2019. PINN immediately took those servers offline and was able to restore most of the data from back-ups. To ensure that PINN's systems were secure and determine if any data was compromised, PINN retained a computer forensics firm to analyze the servers. That firm did not find any evidence that personal information and PHI was accessed or exfiltrated by the attacker, but it also could not rule out the possibility of access or exfiltration. Because the servers at issue contained personal information for PINN patients through April 22, 2019, PINN is erring on the side of caution and concluding that all such information could be at risk. The information potentially at issue could include diagnosis information, names, addresses, dates of birth, and driver's license numbers.

PINN has arranged to provide one year of complimentary credit monitoring and identity theft protection services through ID Experts to the affected patients. Additionally, PINN has established a call center at 833-959-1348 that the affected patients can contact, toll-free, to ask questions and to receive further information regarding the incident. Patients can also enroll in the ID Experts program using that call center.

Notices were sent directly to PINN's current patients. But because of the nature of the data at issue and the historical configuration of PINN's systems, it was not feasible to do a full review of the data and compile a list of affected former patients. Moreover, given that much of the data is several years old, PINN had no way of knowing whether the address information would be accurate. Accordingly, PINN is proceeding with substitute notice under HIPAA and applicable state law. PINN is also notifying the Office of Civil Rights for the Department of Health and Human Services and relevant state regulators (including the Washington Office of the Attorney General) about this incident.

For additional information: PINN is a physical rehabilitation company focused on industrial rehabilitation patients headquartered in Kent, Washington, with a total of seven locations throughout Washington. For more information about this incident, please contact Blaine Kimrey of Vedder Price P.C., 312-609-7810.