

Paul F. Schmeltzer
T (213) 417-5163
F +121348811
Email:pschmeltzer@ClarkHill.com

Clark Hill LLP
555 South Flower Street, 24th Floor
Los Angeles, CA 90071
T (213) 891-9100
F +12134881178

August 15, 2023

Via Electronic Mail

Attorney General Brian E. Frosh
Office of the Attorney General
Identity Theft Unit
200 St. Paul Place
Baltimore, MD 21202
Idtheft@oag.state.md.us

To Whom It May Concern:

We represent Unified Pain Management (“Unified”) with respect to a data security incident involving the potential exposure of limited personally identifiable information (“PII”) described in more detail below. Unified is committed to answering any questions you may have about the data security incident its response and steps taken to prevent a similar incident in the future.

1. Nature of security incident.

On March 21, 2023, Unified learned that there had been unauthorized access to a limited number of its corporate email accounts. Unified conducted an investigation to determine whether any personal information was at risk, but were unable to determine what specific emails or documents were viewed or taken during the period of unauthorized access. Out of an abundance of caution, Unified engaged a vendor to review the emails and documents contained in the email account to identify any personal information that may have been present. Based on the review, Unified determined on July 31, 2023 that some personal information, including a combination of name, address, Social Security number, date of birth, medical diagnosis information, individual health insurance policy number, medical condition or treatment information, and medical record number was present in the files.

2. Number of residents affected.

Three (3) residents of Maryland were affected and notified of the incident. A notification letter was sent to potentially affected individuals on August 16, 2023 (a copy of the template letter is enclosed as Exhibit A).

3. Steps taken or plan to take relating to the incident.

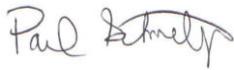
Unified took steps to prevent a similar incident in the future, including changing the passwords for the corporate email accounts, and enabling multi-factor authentication for any remote access to email. In addition, potentially impacted individuals can enroll in twelve (12) months of complimentary credit monitoring and identity restoration services provided by IDX.

4. Contact information.

Unified takes the security of information in its control seriously and is committed to ensuring this information is appropriately protected. If you have any questions or need additional information, please do not hesitate to contact me at pschmeltzer@clarkhill.com or (323) 497-4493.

Sincerely,

CLARK HILL

A handwritten signature in dark ink, appearing to read "Paul Schmeltzer". The signature is fluid and cursive, with the first name "Paul" being more prominent than the last name "Schmeltzer".

Paul Schmeltzer

cc: Jason Schwent

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

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

Enrollment Code: <<ENROLLMENT>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

August 16, 2023

Notice of Data Security Incident

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

We are writing to inform you of a recent data security incident experienced by Unified Pain Management (“Unified”) that may have impacted your personal information described in more detail below. We take the privacy and security of your information seriously, and sincerely apologize for any concern or inconvenience this may cause you. This letter contains information about steps you can take to protect your information and resources we are making available to help you.

What Happened?

On March 21, 2023, Unified learned that there had been unauthorized access to a limited number of its corporate email accounts. We conducted an investigation to determine whether any personal information was at risk, but were unable to determine whether any emails or documents were viewed or taken during the period of unauthorized access. Out of abundance of caution, we engaged a vendor to review the emails and documents contained in the email account to identify any personal information. This process was completed on July 31, 2023, at which point Unified determined that your information may have been present during the period of unauthorized access.

What Information Was Involved?

Impacted information may include some combination of your name, address, Social Security number, date of birth, medical diagnosis information, individual health insurance policy number, medical condition or treatment information, and medical record number.

What We Are Doing

We have taken steps to prevent a similar incident in the future, including changing the passwords for the corporate email accounts, and enabling multi-factor authentication for any remote access to email.

Although we have no evidence your information has been misused, we are providing you with access to credit monitoring and identity protection services provided by IDX. IDX services include: 12 months of Credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do:

While we believe it is unlikely that any of your information will be misused, it is always a good idea to review your credit reports and financial statements for any suspicious activity. You can also visit <https://www.consumer.ftc.gov/topics/privacy-identity-online-security> for more information on how to protect yourself online.

We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 1-888-220-5143, going to <https://app.idx.us/account-creation/protect>, or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 8 am - 8 pm Central Standard Time. Please note the deadline to enroll is November 16, 2023.

Please review the enclosure included with this letter which describes additional steps you can take to help protect your identity, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

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 1-888-220-5143 or go to <https://app.idx.us/account-creation/protect> for assistance or for any additional questions you may have.

Your trust is a top priority for us, and we deeply regret any inconvenience or concern that this matter may cause you.

Sincerely,

Unified Pain Management

Recommended Steps to help Protect your Information.

1. Website and Enrollment. Scan the QR image or 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 1-888-220-5143 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 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
P.O. Box 105069
Atlanta, GA 30348-5069

Equifax Credit Freeze
P.O. Box 105788
Atlanta, GA 30348-5788
1-888-836-6351
www.equifax.com/personal/credit-report-services

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

TransUnion Fraud Reporting
P.O. Box 2000
Chester, PA 19022-2000

TransUnion Credit Freeze
P.O. Box 160
Woodlyn, PA 19094
1-800-680-7289
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) for additional information on protection against identity theft.

District of Columbia: Office of the Attorney General, 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov.

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. You have the right to obtain any police report filed in regard to this incident. There are 0 Rhode Island residents impacted by this 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.