MUNSCH HARDT
DALLAS / HOUSTON / AUSTIN

Ross Tower
500 N. Akard Street, Suite 3800
Dallas, Texas 75201-6659
Main 214.855.7500
Fax 214.855.7584
munsch.com

Direct Dial 2148557591
Direct Fax 214.855.7584
zduffy@munsch.com

October 25, 2023

VIA EMAIL (IDTHEFT@OAG.STATE.MD.US)
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Incident Notification

Dear Sir or Madam:

We are writing on behalf of our client, Medexus Pharma, Inc. ("Medexus"), to notify you of a security incident involving Maryland residents.

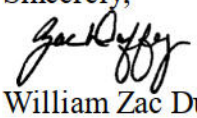
On September 18, 2023, Medexus identified unusual network activity. Medexus immediately took steps to secure the network and began an investigation. The investigation determined that an unauthorized individual had used the credentials of a Medexus employee to remotely access the network and viewed and accessed a file before the IT department severed their access to the systems. Medexus performed a review of the file and concluded that it contained names, phone numbers, and/or addresses together with information about a medical condition (namely, whether a person was potentially a user of or was interested in Medexus's IXINITY product) for 15 Maryland residents.

Medexus expects to begin delivering notifications to Maryland residents on or about October 26, 2023, in substantially the same form as the enclosed letter.

To help prevent something like this from happening again, Medexus implemented additional security measures that included changes as to how multi-factor authentication (MFA) is applied on employee profiles to ensure this setting is active for all employees across the organization. Medexus also intends to conduct a third-party evaluation of its data security systems and practices to confirm that it maintains appropriate levels of data security measures.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,



William Zac Duffy

Enclosure

MEDEXUS PHARMA

October 26, 2023

[Address]
[Address]

Dear Medexus community member –

We value our relationship with you and respect the privacy of your information. Regrettably, we are writing to let you know about an incident that involves your personal information.

On September 18, 2023, an unauthorized individual used the credentials of a Medexus employee to remotely access our network and access a file containing data that had been voluntarily submitted through online forms by users of our websites or, in some instances, communicated directly or otherwise provided to our marketing specialists. We were able to terminate the unauthorized individual's connection to our systems within minutes of discovery. This notification was not delayed as a result of law enforcement investigation. We conducted a review of the file involved and determined that the file included names, phone numbers, and addresses, and included information about your connection to and/or interest in IXINITY, which could indicate a medical condition. The file did not include any passwords, Social Security numbers, or financial records.

We have no indication that any of your information has been misused. We nevertheless take this incident very seriously. We have conducted a thorough review of the affected computer systems. We have also implemented additional security measures designed to prevent something like this from happening again and to protect the privacy of our valued community contacts. As a precaution, we suggest that you review the attachment to this letter for some steps you can consider taking to further protect your information.

We value your privacy and deeply regret that this incident occurred. If you have any questions about this letter, please contact Medexus by phone at 1-855-336-3322, Monday through Friday, between 9:30 am and 4:30 pm Central time, or by email at privacy@medexus.com.

Sincerely,

Michael Adelman
General Manager, US Operations
Medexus Pharma, Inc.

Steps you can take to protect your information

We remind you that it is always a good idea to remain vigilant for attempts or incidents of fraud or identity theft by reviewing your account statements and credit reports for any unauthorized activity.

Monitoring and reporting unauthorized activity

You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows –

> Equifax, PO Box 105281, Atlanta, GA 30348, www.equifax.com, 1-888-378-4329
> Experian, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
> TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe that you have been the victim of identity theft or have reason to believe your personal information has been misused, then you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. (You can obtain information from these sources about steps you can take to avoid identity theft as well as information about fraud alerts and security freezes.) In any such event, we recommend that you also contact your local law enforcement authorities and file a police report. We recommend that you obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. We also recommend that you promptly notify the financial institution or company with which the account is maintained.

Contact information for the Federal Trade Commission is as follows –

> Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

You can also review the FTC's Consumer Information website, a valuable resource with helpful tips on how to protect your information, at https://consumer.ftc.gov/identity-theft-and-online-security.

We also recommend that you review any billing statements you receive from your health insurer or healthcare provider. If you see charges for services you did not receive, then you should immediately contact the insurer or provider.

Fraud alerts and credit or security freezes

Fraud alerts

There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may place an initial fraud alert on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may place an extended alert on your credit report if you have already been a victim of identity theft and can provide appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years unless you ask them not to do so.

Credit or security freezes

You have the right to place a credit freeze, also known as a security freeze, on your credit file, free of charge. Doing so makes it more difficult for identity thieves to open new accounts in your name because most creditors need to see your credit report before they approve a new account. If they cannot see your report, then they may not extend the credit.

There is no fee to place or lift a security freeze on your credit reports. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the following addresses –

Experian Security Freeze, PO Box 9554, Allen, TX 75013, www.experian.com
TransUnion Security Freeze, PO Box 2000, Chester, PA 19016, www.transunion.com
Equifax Security Freeze, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You will need to supply your name, address, date of birth, Social Security number, and other personal information. After receiving your freeze request, each credit bureau will provide you with a unique personal identification number (or PIN) or password. Keep the PIN or password in a safe place. You will need it in the event you choose to lift the freeze.

A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, then a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after they receive your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, then you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you will need to make the request with all three credit bureaus.

Additional information

You may contact Medexus Pharma, Inc. at: 29 North Wacker Drive, Suite 704, Chicago, Illinois 60606, Phone: 1-855-336-3322, Email: privacy@medexus.com, Website: www.medexus.com.

District of Columbia residents may contact and obtain information from your attorney general at: Office of the Attorney General for the District of Columbia, 440 6th Street, NW, Washington, DC 20001, Phone: 1-202-727-3400, Email: oag@dc.gov, Website: www.oag.dc.gov.

Maryland residents may contact and obtain information from your state attorney general at: Maryland Attorney General's Office, 200 St. Paul Place, Baltimore, MD 21202, Phone: 1-888-743-0023 / 1-410-576-6300, Email: consumer@oag.state.md.us, Website: www.oag.state.md.us.