

14637

From: Brian Beidelman <BrianBeidelman@acaciapharma.com>
Sent: Sunday, March 03, 2019 11:32 AM
To: [REDACTED]
Subject: Formal Data Breach Notification



Acacia Pharma Inc.
8440 Allison Pointe Blvd. Suite 100
Indianapolis, Indiana 46250
The United States

March 3, 2019

RE: Notice of Data Breach,

Dear [REDACTED]

As we initially alerted you in our email of February 26, 2019, Acacia Pharma Inc. (“Acacia”) was the victim of a February 25, 2019 data security incident in which US employee, personally identifiable information was phished via an email scam. Acacia is writing to provide you with further notification regarding this security incident that may impact your personal information.

Although we are unaware of any actual or attempted misuse of your information, we are providing you with information regarding the incident, steps we have taken since discovering the incident, and what you can do to protect against identity theft should you wish to do so.

What Happened? Acacia has determined that an employee accidentally disclosed certain personal information to an unauthorized attacker in response to a phishing email. Specifically, on February 25, 2019, our employee sent information pertaining to approximately 35 US-based Acacia employees to an unauthorized actor posing as an Acacia executive. The employee disclosed the information in an email mistakenly believing they were responding to a legitimate inquiry by Acacia’s Chief Financial Officer and Secretary. Our employee learned the email was a phishing attack when the attacker responded to the initial email and requested specific employee W-2 information. The employee did not respond to this second email from the attacker, did not provide the employee W-2 information requested, and reported the phishing attack immediately after learning the initial email was not legitimate.

What Information Was Involved? The information related to you sent within the email included your name, social security number, and your 2018 earned wage, and tax withholding information. We can confirm the email was sent, and can reasonably assume that your personal and financial information was received and accessed by the phishing attacker.

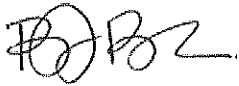
What We Are Doing. Acacia has no indication at this time that any fraud has resulted from this incident. We have heightened our awareness and established internal protocols in an effort to prevent any such incidents from occurring in the future.

What You Can Do. Please review the enclosed “*Steps You Can Take to Prevent Identity Theft and Fraud.*” In addition, we advise you to report any suspected incidents of identity theft to local law enforcement or State Attorney General.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. We ask that you please contact Brian Beidelman, Human Resources Director at (317) 979-8780 or brianbeidelman@acaciapharma.com with any questions regarding this incident.

On behalf of Acacia, we apologize for any inconvenience this incident may cause. Like many companies, our business is under constant attack from bad actors and we must all remain vigilant to help ensure we do not fall victim to further attacks. Should you ever have any questions regarding data security, please do not hesitate to contact the above.

Sincerely,



Brian Beidelman
Human Resources Director
Acacia Pharma Inc.

Steps You Can Take to Protect Against Identity Theft and Fraud

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a “*security freeze*” on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian
PO Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/freeze/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016
1-800-909-8872

www.transunion.com/credit-freeze

Equifax
PO Box 105788
Atlanta, GA 30348-5788
1-800-685-1111

www.equifax.com/personal/credit-report-services

In order to request a security freeze, you may need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number; and
3. Date of birth.

As an alternative to a security freeze, you have the right to place an initial or extended “fraud alert” on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian
P.O. Box 2002
Allen, TX 75013
1-888-397-3742

www.experian.com/fraud/center.html

TransUnion
P.O. Box 2000
Chester, PA 19106
1-800-680-7289

www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008

www.equifax.com/personal/credit-report-services

Although we have no reason to believe that your personal information has been used to file fraudulent tax returns, you can contact the IRS at www.irs.gov/Individuals/Identity-Protection for helpful information and guidance on steps you can take to address a fraudulent tax return filed in your name and what to do if you become the victim of such fraud. You can also visit www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information.

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 Illinois residents, the Federal Trade Commission can be contacted at 600 Pennsylvania Avenue, NW Washington, DC 20580, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261, www.identitytheft.gov.

For Maryland residents, you can obtain information about steps he can take to avoid identity theft from the Office of the Maryland Attorney General and Federal Trade Commission. The Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us; the Federal Trade Commission can be contacted at 600 Pennsylvania Avenue, NW Washington, DC 20580, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261, www.identitytheft.gov.