C/O ID Experts
PO Box 4219
Everett WA 98204

ENDORSE

A FIRST NAME LAST NAME
ADDRESS1
ADDRESS2
CSZ BREAK
SEQ
CODE 2D COUNTRY

August 5, 2019

**Notice of Data Breach**

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

I am writing to let you know that a third party vendor (the "vendor") has notified Amarin Pharma, Inc. ("Amarin") about a security matter involving a database maintained by the vendor that may have contained certain information about you. According to the vendor, this database does not contain your financial account information, credit card information, or Social Security number, but it may include your name, address, and your interest in a copay card for Vascepa®, an Amarin product. The vendor is an independent company that supports Amarin's copay assistance programs by providing customer relationship management services relating to Vascepa®. Amarin's systems were not affected by this incident. At this time, we have no reason to believe that your data has been misused for fraud or identity theft.

**What Happened**

On or around June 20, 2019, we became aware of media reports suggesting that a database containing information about consumers who use or have expressed interest in Vascepa® may have been subject to unauthorized access. Amarin promptly began investigating these reports and determined that the database in question was maintained by the vendor. Amarin promptly took steps to suspend active data feeds to the vendor's database, and the vendor informed us that the database was taken offline on June 20, 2019.

On July 11, 2019, the vendor informed us that due to a database misconfiguration, information could have been accessed without proper authorization between May 2, 2018, and June 20, 2019. The vendor further informed us that it identified evidence of unauthorized access to and acquisition of information from the database during the period May 29, 2019 to June 20, 2019, and that it could not conclusively determine that no unauthorized access or acquisition occurred outside this timeframe. We are not certain whether your specific data was accessed or acquired and are not aware of your data being misused for fraud or identity theft.

**What Information Was Involved**

According to the vendor, information in the database subject to unauthorized access and acquisition included names, postal and email addresses, phone numbers, and information about consumers' use of certain supplements or medications, including Vascepa®. The database also contained information about certain copay transactions for Vascepa®, including dates the transactions were completed. The vendor confirmed the database did not contain Social Security numbers or financial account information.

**What We Are Doing**

We are notifying you about this matter so that you can, if desired, take precautions to protect yourself. We have taken steps to assure that the vendor's database is secure from further unauthorized access. In addition, we have taken steps to ensure that any copay cards for Vascepa® accessed from the vendor-supported website remain active for continued use. Use of the copay card program has not been interrupted.

We are working with our vendor and leading experts to confirm the scope of this matter. The vendor has informed us that it engaged a forensic investigator to evaluate the security of its systems. We will not authorize bringing the database back online until we have confirmed that appropriate safeguards are in place.

**What You Can Do**

Although we do not believe that any financial information was in the vendor's database, we recommend that you remain vigilant for incidents of fraud and identity theft. As a precaution to protect against potential misuse of your health information, we recommend that you regularly monitor any explanation of benefits statements that you receive from your health plan to check for any unfamiliar health care services. If you notice any health care services that you did not receive listed on any of these statements, please contact your health plan.

We also recommend that you periodically check your credit report from one or more of the national credit reporting agencies. You are entitled to obtain a free annual credit report from each of the nationwide credit reporting companies—Equifax, Experian, and TransUnion. To do so, please go to www.annualcreditreport.com or call 1-877-322-8228. If you notice any suspicious activity, you should promptly report such activity to the proper law enforcement agencies, including your state Attorney General and the Federal Trade Commission ("FTC").

You may also consider placing a fraud alert on your credit files. Adding a fraud alert to your credit report file makes it more difficult for someone to get credit in your name by requiring creditors to follow certain procedures. However, this may also delay your ability to obtain credit. No one is allowed to place a fraud alert on your credit report except you, so if you elect to do so, please contact one of the three nationwide credit reporting agencies. Note that the first agency that processes your fraud alert will notify the others to do so as well. You may also add a security freeze to your credit report file to prohibit a credit reporting agency from releasing information from your credit report without your prior written authorization. Agencies are required to place or remove credit freezes free of charge. You can obtain information on fraud alerts and security freezes from the consumer reporting agencies and the FTC.

| **Equifax** | **Experian** | **TransUnion** |
|---|---|---|
| Fraud Victim Assistance | National Consumer Assistance | Fraud Victim Assistance |
| P.O. Box 740256 | P.O. Box 9554 | P.O. Box 2000 |
| Atlanta, GA 30374 | Allen, TX 75013 | Chester, PA 19016 |
| www.equifax.com | www.experian.com | www.transunion.com |
| 1-800-525-6285 | 1-888-397-3742 | 1-800-680-7289 |

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report and promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state Attorney General, and/or the FTC.

You may contact the FTC or your state Attorney General to obtain additional information about avoiding identity theft.

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

You can find information on how to contact your state Attorney General at: www.naag.org/naag/attorneys-general/whos-my-ag.php.

**For More Information**

If you have any questions or concerns that are not addressed in this letter, you may contact us by visiting https://ide.myidcare.com/amarin or calling 1-833-300-6932 from 9 a.m. to 9 p.m. Eastern Time Monday through Friday to speak with a representative.

Sincerely,

Dan S. Dunham
SVP, Chief Pharmaceutical Compliance Officer
Amarin Pharma, Inc.

SEQ
CODE 2D