July 2, 2021

BY ONLINE SUBMISSION

Office of the Attorney General
6 State House Station
Augusta, ME 04333

To Whom It May Concern:

On behalf of Envision Pharma Group Ltd. (together with its subsidiaries, "Envision"), and pursuant to 10 M.R.S.A. § 1348, this letter provides notice of a cybersecurity incident. Envision is a service provider in the medical affairs and healthcare communications industry.

In late January 2021, Envision experienced a ransomware incident and after an extensive investigation and eDiscovery process, we recently discovered that one Maine resident was affected by the incident, which is the basis of this notice.

On or about January 26, 2021, Envision was alerted by its managed detection and response provider of suspicious activity on its network and subsequently discovered that a third party had gained unauthorized, remote access to Envision's internal Envision Pharma Group (EPG) corporate and Envision Scientific Services (ESS) networks ("Envision's Environment"). The earliest known date of unauthorized third party activity in Envision's Environment was on January 19, 2021. There has been no observed malicious activity in Envision's Environment since January 26, 2021. The separate Envision Technology Solutions client hosting environment, in which the vast majority of Envision's clients' data is housed was not affected by the incident. Envision also reported the incident to law enforcement.

After becoming aware of the incident, Envision promptly took steps to prevent further unauthorized access and began a thorough investigation with the support of outside cybersecurity experts, which determined that the unauthorized third party had acquired a copy of certain information stored in Envision's Environment. Due to the nature of the incident, it was unclear for some time what kinds of data were affected and the extent to which it involved personal data. Since February, Envision has been diligently conducting a detailed eDiscovery review of the documents and information accessed by the threat actor, which included a number of steps and a manual review of a significant number of documents. It was only recently that we have identified one (1) Maine resident whose personal information was part of the data acquired.

The types of information acquired by the unauthorized third party included the affected individual's Social Security Number. Envision is not aware of any cases of identity theft, fraud, or financial losses to individuals stemming from this incident and does not believe the unauthorized third party was targeting personal information in the incident.

Envision sent this individual formal notice on July 2, 2021 via U.S. Mail. A sample individual notification letter is enclosed. As stated in the attached sample notice, to protect the affected individual further, Envision is offering to provide 24 months of free identity theft and credit monitoring services through Equifax. Envision has also established a call center to respond to individuals' questions.

Since discovering the incident, Envision is continuing to monitor and improve its capabilities to detect any further threats and avoid any future unauthorized activity. Specifically, Envision has performed multiple external vulnerability scans, and widely deployed additional endpoint security monitoring technologies across Envision's IT environment to ensure all systems were brought back online safely. Envision has also performed a dark web search and has engaged in continuous monitoring, neither of which has found compromised Envision data. Envision regularly evaluates its security protocols and procedures to ensure that data is protected as a matter of course. Following the incident, Envision has also reviewed and reinforced this process to ensure the ongoing security of its systems.

Envision takes the protection of personal information of all of its stakeholders seriously and is committed to answering any questions that your office may have. Please do not hesitate to contact me at +44 (0) 208 834 3931 or arthur.shih@envisionpharma.com.

Respectfully yours,

Arthur Shih
General Counsel

Enclosure

ENVISION PHARMA GROUP
Driven by evidence, enabled by technology

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

[redacted]

July 2, 2021

NOTICE OF SECURITY INCIDENT

Dear [redacted],

We are writing regarding a cybersecurity incident that occurred at Envision Pharma Group, Ltd ("Envision"). We want to make clear at the outset that keeping personal data safe and secure is very important to us, and we deeply regret that this incident occurred.

WHAT HAPPENED?

On or about January 26, 2021, we learned that an unauthorized third party had gained remote access to certain internal Envision computer networks in an effort to disrupt our operations. We quickly took steps to secure our network and began to investigate the incident with the support of outside cybersecurity experts. We have determined that the unauthorized third party acquired some non-public data from our networks. We recently learned that certain of your information was affected.

WHAT INFORMATION WAS INVOLVED?

Based on our review, the personal information acquired by the unauthorized third party related to the period from 2011 to 2012 and consisted of your [redacted]. However, Envision currently has no knowledge that your information has been misused and does not believe the unauthorized third party was targeting personal information in the incident. The information relating to you was held by Envision for the purposes of services provided by Envision to affiliated companies whilst Envision was owned by United BioSource Corporation, including your employer at the time.

WHAT WE ARE DOING

We took prompt steps to address this incident, including contacting law enforcement and engaging outside cybersecurity experts to help remediate and ensure the ongoing security of our systems. As part of our ongoing efforts to ensure the security of our systems, we have enhanced cybersecurity protections throughout our environment.

We have also secured the services of Equifax to provide identity and credit monitoring services at no cost to you for two years. Below please find information on signing up for a complimentary two-year membership to Equifax Credit Watch Gold, which helps detect misuse of your personal information and provides you with identity protection focused on identification and resolution of identity theft.

t: +44 (0) 1403 322 000
info@envisionpharmagroup.com
envisionpharmagroup.com

July 2, 2021

Activation Code: [redacted]

Expiration Date: [redacted]

Equifax Credit Watch Gold

*Note: You must be over age 18 with a credit file to take advantage of the product.

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications[1] when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts[2], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[3]
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft[1]

Enrollment Instructions

To sign up online for online delivery, go to www.equifax.com/activate

Enter your unique Activation Code of [redacted] then click "Submit" and follow these 4 steps:

1. **Register:** Complete the form with your contact information and click "Continue". If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4.
2. **Create Account:** Complete the form with your email address, create a password, and accept the Terms of Use.
3. **Verify Identity:** To enroll in your product, the system will ask you to complete an identity verification process.
4. **Checkout:** Upon successful verification of your identity, you will see the Checkout Page. Click 'Sign Me Up' to finish enrolling. The confirmation page shows your completed enrollment. Please click the "View My Product" button to access the product features.

You need to activate your membership in order to receive your benefits, and must do so no later than [redacted]. **Your Activation Code will not work after this date**.

If you have questions about our provision of this complementary credit monitoring service to you, please contact Equifax at **(888) 548-7878**.

---

[1] WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded.

[2] The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.

[3] Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com.

[4] The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

July 2, 2021
Activation Code: [redacted]
Expiration Date: [redacted]

WHAT YOU CAN DO

We strongly encourage you to contact Equifax and take advantage of the credit monitoring and identity theft protection services we are providing to you free of charge. Remain vigilant and carefully review your accounts for any suspicious activity.

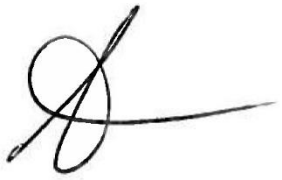
If you detect any suspicious activity on an account, you should change the password and security questions associated with the account, and promptly notify the financial institution or company with which the account is maintained and any relevant government agency, such as IRS, SSA, or state DMV, as applicable.

If you would like to take additional steps to protect your personal information, attached to this letter are helpful resources on how to do so, 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

We take our responsibility to protect your information extremely seriously, and sincerely regret any inconvenience that this unfortunate incident has caused you. If you have any questions regarding this incident, you may contact Envision directly at Privacy@EnvisionPharma.com for further information.

Sincerely,



John Gillie
Chief Financial & Operating Officer
On behalf of Envision Pharma Group, Ltd

Additional Resources

Below are additional helpful tips you may want to consider to protect your personal information.

Review Your Credit Reports and Account Statements; Notify Law Enforcement of Suspicious Activity

As a precautionary measure, we recommend that you remain vigilant by reviewing your credit reports and account statements closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact law enforcement, the Federal Trade Commission ("FTC") and/or the Attorney General's office in your home state. You can also contact these agencies for information on how to prevent or avoid identity theft. You can contact the FTC at:

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

Copy of Credit Report

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting https://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to the Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can print this form at https://www.annualcreditreport.com/manualRequestForm.action. Credit reporting agency contact details are provided below.

Equifax:	**Experian**:	**TransUnion**:
equifax.com equifax.com/personal/credit-report-services P.O. Box 740241 Atlanta, GA 30374 866-349-5191	experian.com experian.com/help P.O. Box 2002 Allen, TX 75013 888-397-3742	transunion.com transunion.com/credit-help P.O. Box 1000 Chester, PA 19016 888-909-8872

When you receive your credit reports, review them carefully. Look for accounts or credit inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is inaccurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Fraud Alert

You may want to consider placing a fraud alert on your credit file. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. If you have already been a victim of identity theft, you may have an extended alert placed on your report if you provide the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above.

Security Freeze

You have the right to place a security freeze on your credit file free of charge. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. As a result, using a security freeze may delay your ability to obtain credit. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name; social security number; date of birth; current and previous addresses; a copy of your state-issued identification card; and a recent utility bill, bank statement or telephone bill.

Federal Fair Credit Reporting Act Rights

The Fair Credit Reporting Act (FCRA) is federal legislation that regulates how consumer reporting agencies use your information. It promotes the accuracy, fairness, and privacy of consumer information in the files of consumer reporting agencies. As a consumer, you have certain rights under the FCRA, which the FTC has summarized as follows: you must be told if information in your file has been used against you; you have the right to know what is in your file; you have the right to ask for a credit score; you have the right to dispute incomplete or inaccurate information; 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 reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; you may seek damages from violators. Identity theft victims and active duty military personnel have additional rights.

For more information about these rights, you may go to www.ftc.gov/credit or write to: Consumer Response Center, Room 13-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

Additional Information

You have the right to obtain any police report filed in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

You may consider starting a file with copies of your credit reports, any police report, any correspondence, and copies of disputed bills. It is also useful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.

For Colorado, Delaware, and Illinois residents: You may obtain information from the federal trade commission and the credit reporting agencies about fraud alerts and security freezes.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Maryland residents: You may contact the Office of the Maryland Attorney General, 200 St. Paul Place, Baltimore, MD 21202, http://www.marylandattorneygeneral.gov/, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27699-9001, http://www.ncdoj.gov/, 1-877-566-7226. You are also advised to report any suspected identity theft to law enforcement or to the North Carolina Attorney General.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the Oregon Attorney General.

For Georgia, Maryland, New Jersey, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit bureaus directly to obtain such additional report(s).

For New York residents: You may contact the New York Office of the Attorney General at: The Capitol, Albany, NY 12224-0341, http://www.ag.ny.gov/home.html, 1-800-771-7755, and the New York Department of State Division of Consumer Protection at: 99 Washington Avenue, Albany, New York 12231-0001, http://www.dos.ny.gov/consumerprotection, 1-800-697-1220.

For Rhode Island residents: You may obtain information from the federal trade commission and the credit reporting agencies about fraud alerts and security freezes. You may also contact the Rhode Island Office of the Attorney General, 150 South Main Street Providence, Rhode Island 02903, http://www.riag.ri.gov/, (401) 274-4400.