Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

October 11, 2024

M2014-L03-0000001 T00001 P001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L03
APT ABC
123 ANY STREET
ANYTOWN, FC 1A2 B3C
COUNTRY

**Re: Notice of Data Security Incident**

Dear Sample A. Sample:

Wellfleet Group, LLC ("Wellfleet") is a third party administrator for Wellfleet Insurance Company and Wellfleet New York Insurance Company that provides health insurance solutions and services to the students of post-secondary education institutions (e.g., colleges and universities) ("Schools"). Wellfleet also supports administration of these health plans in various ways. Due to the nature of this work, Wellfleet is provided access to certain personal information of the students to perform these services.

We are writing to inform you that we experienced a data security incident that involved some of your protected health information associated with medical referrals made during your participation in your current or former School's student health plan. As noted above, Wellfleet was in possession of this information due to its work as the administrator for your School's student health plan. This notice explains the incident, steps we have taken in response, and additional information on steps you may take to help protect your information.

***What happened?***

On August 1, 2024, Wellfleet became aware that a student's medical referral was accessible online via a common Internet search engine. Wellfleet immediately began an investigation into this issue and engaged leading third-party experts to investigate the scope of and remediate the problem.

The investigation determined that a previously unknown misconfiguration on Wellfleet's website ("Website") allowed deep-links to the medical referral print page ("Referral(s)") of users to be accessible without authentication, which then enabled web crawlers of various Internet search engines to scrape the Referrals and index them. In some instances, these indexed Referrals were available as a search result in response to searching for the relevant student's name ("Publicly Accessible Referrals").

Wellfleet immediately took steps to disable this misconfiguration, remove the Referrals from the Internet, and identify any other misconfigurations with the Website. We also conducted a thorough review of that data to identify what information was involved and identify individuals to whom the data related.

Importantly, the investigation also confirmed that this issue was not the result of a cyber-attack or related to any type of malicious cyber activity, and that further, this incident was limited to the Website and did not impact the functioning of any of Wellfleet's products or other systems or networks.

***What information was involved?***

The review determined that your specific Referral(s) were included as part of the set of Publicly Accessible Referrals, and the data involved contained some of your protected health information, including your name, and one or more of the following: full name, mailing address, phone number, date of birth, insurance group/policy number, school ID number, and health/medical information (e.g., reason for referral and diagnosis code). As noted below, Wellfleet found and either removed or blocked public access to all Publicly Accessible Referrals, so your Referral(s) that were involved are no longer publicly accessible.

***What are we doing?***

First, as noted above, Wellfleet immediately disabled the misconfiguration and was able to find and remove or block public access to all the Publicly Accessible Referrals. Additionally, Wellfleet also started a full review and evaluation of the Website to ensure that there were no other problems or misconfigurations. Wellfleet also updated and reset data security controls for the Website. Further, we are also revamping our standard review and technical support of all applications and software development processes to help prevent similar incidents from occurring in the future.

***What can you do?***

As noted above, we found and either removed or blocked public access to all Publicly Accessible Referrals, so your Referral(s) that were involved are no longer publicly accessible. Additionally, when your Referral(s) was publicly accessible, it would have required someone searching for specific information contained within the Referral(s), such as your full name within the Referral(s) to find and access such Referral(s), which we believe limits the potential access to the same. Thus, while we are not aware of any evidence that your protected health information has been misused, we wanted to make you aware of the incident and provide you with additional information on steps you may consider taking. We encourage you to remain vigilant of your information and, as a precaution, **Wellfleet is offering you complimentary credit monitoring and fraud prevention services through Experian Identity Works ("IdentityWorks") for 24 months**. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. IdentityWorks is completely free to you and enrolling in this program will not hurt your credit score.

For more information on Experian IdentityWorks℠, including instructions on how to activate your complimentary 24-month membership, as well as additional steps you may take to help protect your information, please see the additional information provided in the following pages.

***For more information.***

Wellfleet takes the security of personal information seriously, and sincerely regrets that this incident occurred. For more information, or if you have any questions or need additional information, please call 833-931-3700, Monday through Friday, between 9:00 a.m. and 9:00 p.m. Eastern Time (excluding major U.S. holidays). Please be prepared to provide engagement number [redacted] If you have a speech or hearing impairment and use a TTY, please dial 711.

Sincerely,

Wellfleet

## Experian IdentityWorks Enrollment Information

To help protect your identity, we are offering complimentary access to Experian IdentityWorks[SM] for 24 months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks[SM] as a complimentary 24-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** January 31, 2025 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/credit
- Provide your **activation code**: ABCDEFGHI

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 833-931-3700 by January 31, 2025. Be prepared to provide engagement number [redacted] as proof of eligibility for the Identity Restoration services by Experian.

### ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE[TM]:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

## Information About Identity Theft Protection Guide

**Contact information for the three nationwide credit reporting companies is as follows:**

| Equifax | Experian | TransUnion |
|---|---|---|
| Phone: 1-800-685-1111<br>P.O. Box 740256<br>Atlanta, Georgia 30348<br>www.equifax.com | Phone: 1-888-397-3742<br>P.O. Box 9554<br>Allen, Texas 75013<br>www.experian.com | Phone: 1-888-909-8872<br>P.O. Box 105281<br>Atlanta, GA 30348-5281<br>www.transunion.com |

**Free Credit Report.** We remind you to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. If you identify any unauthorized charges on your financial account statements, you should immediately report any such charges to your financial institution. 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, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

**For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, 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 reporting agencies directly to obtain such additional report(s).

**Security Freeze.** Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too.

How will these freezes work? Contact all three of the nationwide credit reporting agencies – Equifax, Experian, and TransUnion. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee.

The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement.

It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

**For New Mexico residents:** You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

**Fraud Alerts.** A fraud alert tells businesses that check your credit that they should check with you before opening a new account. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the 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.

**Federal Trade Commission and State Attorneys General Offices.** 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 the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft. You may contact the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

**For Connecticut residents:** You may contact and obtain information from your state attorney general at: Connecticut Attorney General's Office, 55 Elm Street, Hartford, CT 06106, 1-860-808- 5318, www.ct.gov/ag

**For District of Columbia residents:** You may contact the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001, https://oag.dc.gov, 202-442-9828.

**For Maryland residents:** You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743- 0023**.**

**For New York residents:** You may contact the New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1- 800-697- 1220, http://www.dos.ny.gov/consumerprotection; and New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov.

**For North Carolina residents**: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

**For Rhode Island residents:** You may contact the Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, http://www.riag.ri.gov, 401-274-4400**.**

**Reporting of Identity Theft and Obtaining a Police Report.** You have the right to obtain any police report filed in the United States 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.

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

**For Massachusetts residents:** You have the right to obtain a police report if you are a victim of identity theft. You also have a right to file a police report and obtain a copy of it.

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

**For Rhode Island residents:** You have the right to file or obtain a police report regarding this incident. 50 Rhode Island residents were impacted by this incident.