



150 N. Riverside Plaza, Suite 3000, Chicago, IL 60606 • (312) 819-1900

October 20, 2022

Bruce A. Radke
312.463.6211
312.873.3763 Fax
bradke@polsinelli.com

VIA E-MAIL (ATTORNEYGENERAL@DOJ.NH.GOV)

The Honorable John M. Formella
Attorney General of the State of New Hampshire
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notification of a Potential Data Security Incident

Dear Attorney General Formella:

We represent Seattle Cancer Care Alliance, which is now known as Fred Hutchinson Cancer Center (“Fred Hutch”) in connection with a recent incident that may have involved the Personal Information of one New Hampshire resident. Fred Hutch is reporting the incident pursuant to N.H. Rev. Stat. § 359-C:19 *et. seq.* This notice will be supplemented, if necessary, with any new significant facts discovered subsequent to this submission. While Fred Hutch is notifying you of this incident, Fred Hutch does not waive any rights or defenses relating to the incident, this notice, or the applicability of New Hampshire law on personal jurisdiction.

NATURE OF THE INCIDENT

On or about March 26, 2022, Fred Hutch identified suspicious activity associated with one (1) employee’s business email account (the “Account”). Fred Hutch immediately terminated any access to the Account, and forced a credential reset to eject any suspected unauthorized individuals from the Account. Fred Hutch also engaged a leading forensic security firm to further investigate and to confirm the security of its email and computer systems. The forensic investigation concluded on or about April 18, 2022 and determined that an unauthorized third party gained access to the Account between March 25 and March 26, 2022. Thereafter, Fred Hutch reviewed the Account’s contents to determine if it contained any Personal Information and, on September 9, 2022, determined that it contained Personal Information for a single resident of New Hampshire.

The investigation did not find evidence confirming that the unauthorized party actually viewed any personal information in the account, nor have there been any instances of actual or attempted fraud against a patient. Nevertheless, because there was an email account compromise and Fred

polsinelli.com

Atlanta Boston Chicago Dallas Denver Houston Kansas City Los Angeles Miami Nashville New York
Phoenix St. Louis San Francisco Seattle Silicon Valley Washington, D.C. Wilmington

Polsinelli PC, Polsinelli LLP in California

86110343.3



October 20, 2022

Page 2

Hutch cannot isolate exactly what, if any, information may have been viewed, Fred Hutch is notifying the individuals whose personal information was contained in the account.

NUMBER OF NEW HAMPSHIRE RESIDENTS AFFECTED

On September 9, 2022, Fred Hutch determined that the name, Social Security number, and financial account information of one resident was contained in the Account. Fred Hutch is mailing notification letters to these individuals today, October 20, 2022, via first-class United States mail. The notification letters include an offer for twelve (12) months of complimentary credit monitoring and identity theft protection for any individual whose Social Security, government ID, or driver's license number was included in the Account. Enclosed is a template copy of the notice that is being mailed.

STEPS TAKEN RELATING TO THE INCIDENT

Upon learning of the incident, Fred Hutch promptly secured the involved email account to prevent further access. It also conducted a comprehensive search for any personal information in the email account and retained a leading forensic security firm to investigate and confirm the security of its email and computer systems. Fred Hutch is undertaking efforts to reduce the risk of a similar incident occurring in the future, including implementing new technical safeguards and retraining workforce. Fred Hutch provided a preliminary notification to the Department of Health & Human Services Office for Civil Rights ("HHS-OCR") on May 25, 2022, and is supplementing its report today, October 20, 2022. Finally, as discussed above, Fred Hutch is notifying the involved individuals and providing any living individuals whose Social Security number was exposed with an offer for one-year of complimentary credit monitoring and identity theft protection.

CONTACT INFORMATION

Please do not hesitate to contact me if you have any questions or if I can provide you with any further information concerning this matter.

Sincerely,

Bruce A. Radke

Enclosure



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

NOTICE OF DATA BREACH

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Seattle Cancer Care Alliance, which is now known as Fred Hutchinson Cancer Center ("Fred Hutch"), is committed to the privacy of individuals and takes the protection of personal information that is entrusted to us seriously. Unfortunately, we are writing to make you aware of a recent data security incident that may have involved some of your personal information.

What Happened. On March 26, 2022, we discovered suspicious activity associated with a single employee's business email account. Upon learning of the situation, we contained the incident by securing the account to prevent further access, immediately began an internal investigation, and retained a leading forensic cybersecurity firm to aid in our investigation of the incident and confirm the security of our computer systems. The forensic investigation concluded on or about April 18, 2022 and determined that an unauthorized individual accessed the account between March 25 and March 26, 2022. In order to identify which individuals' information was contained in the account, we engaged a specialized document review team to conduct a comprehensive review of the contents of the email account. After that review was completed, we searched for and confirmed contact information for those individuals whose sensitive information was contained in the account.

What Information Was Involved. While we did not see any evidence to suggest that the unauthorized individual was trying to view patient information, we reviewed the entire email account for personal information. On September 9, 2022, our investigation confirmed that the account contained your <<b2b_text_1(name, data elements)>><<b2b_text_2(data elements cont.)>>.

What We Are Doing. As soon as we observed the suspicious activity, Fred Hutch immediately worked to secure the account. Throughout the investigatory process, Fred Hutch notified and cooperated with federal law enforcement, worked with teams of experts to identify the nature and scope of any unauthorized access, and worked diligently to identify and notify individuals as appropriate. Additionally, we have taken steps to help prevent a similar incident from occurring in the future. We have notified federal law enforcement of the incident.

Although we are not aware of any instances of fraud or identity theft involving your information, we are offering you a complimentary one-year membership of Experian IdentityWorksSM. 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. IdentityWorksSM is completely free to you and enrolling in this program will not hurt your credit score. **For more information on identity theft prevention and IdentityWorks, including instructions on how to activate your complimentary, one-year membership, please see the additional information attached to this letter.**

What You Can Do. You can find more information on steps to protect yourself against identity theft or fraud in the enclosed *Additional Important Information* sheet. We also recommend that you enroll in the complimentary credit monitoring services that are being offered.

For More Information. For further information and assistance, please call [1-800-422-6237](tel:1-800-422-6237) from 6:00 a.m. to 3:30 p.m. PST, Monday through Friday (excluding some U.S. holidays).

We value the trust you place in us and take our responsibility to safeguard your personal information seriously. We apologize for any inconvenience or concern this incident might cause.

Sincerely,

Shauna Van Dongen
Director, Compliance, Ethics & Integrity, Fred Hutchinson Cancer Center

ACTIVATING YOUR COMPLIMENTARY CREDIT MONITORING

To help protect your identity, we are offering a **complimentary** one-year membership of Experian IdentityWorksSM Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: <<b2b_text_6(activation deadline)>> (Your code will not work after this date.)
2. Visit the **Experian IdentityWorks website** to enroll: <https://www.experianidworks.com/3bcredit>
3. PROVIDE the **Activation Code**: <<activation code s_n>>

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-288-8057. Be prepared to provide engagement number <<b2b_text_3(engagement number)>> as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

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, Equifax and Transunion files 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™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Activate your membership today at <https://www.experianidworks.com/3bcredit> or call 877-288-8057 to register with the activation code above.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-288-8057.

* 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.

Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports 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 should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Credit Reports: You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at <https://www.annualcreditreport.com/manualRequestForm.action>.

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax
1-866-349-5191
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

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

TransUnion
1-800-888-4213
www.transunion.com
P.O. Box 2000
Chester, PA 19016

Fraud Alerts: You may want to consider placing a fraud alert on your credit report. A fraud alert is free and will stay on your credit report for one (1) year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at www.annualcreditreport.com.

Credit and Security Freezes: You may have the right to place a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A credit freeze can be placed without any charge and is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax Security Freeze
1-888-298-0045
www.equifax.com
P.O. Box 105788
Atlanta, GA 30348

Experian Security Freeze
1-888-397-3742
www.experian.com
P.O. Box 9554
Allen, TX 75013

TransUnion Security Freeze
1-888-909-8872
www.transunion.com
P.O. Box 160
Woodlyn, PA 19094

This notification was not delayed by law enforcement.

Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/documents/bcftp_consumer-rights-summary_2018-09.pdf, or by requesting information in writing from the Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

Iowa Residents: Iowa residents can contact the Office of the Attorney general to obtain information about steps to take to avoid identity theft from the Iowa Attorney General's office at: Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines IA 50319, 515-281-5164.

Maryland Residents: Maryland residents can contact the Office of the Attorney General to obtain information about steps you can take to avoid identity theft from the Maryland Attorney General's office at: Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, (888) 743-0023, <http://www.marylandattorneygeneral.gov/>.

New York State Residents: New York residents can obtain information about preventing identity theft from the New York Attorney General's Office at: Office of the Attorney General for the State of New York, Bureau of Consumer Frauds & Protection, The Capitol, Albany, New York 12224-0341; <https://ag.ny.gov/consumer-frauds/identity-theft>; (800) 771-7755.

North Carolina Residents: North Carolina residents can obtain information about preventing identity theft from the North Carolina Attorney General's Office at: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov.

Rhode Island Residents: We believe that this incident affected 20 Rhode Island residents. Rhode Island residents can contact the Office of the Attorney general at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. You have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Vermont Residents: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).