David McMillan, Partner
Cybersecurity & Data Privacy Team
175 Pearl Street, Suite C-402
Brooklyn, NY 11201
dmcmillan@constangy.com
Mobile: 718.614.8371

May 25, 2023

VIA ONLINE SUBMISSION
Attorney General Aaron Frey
Office of the Attorney General
Consumer Protection Division
Security Breach Notification
111 Sewall Street, 6th Floor
Augusta, ME 04330

Re: **Notice of Data Security Incident**

Dear Attorney General Frey:

Constangy, Brooks, Smith & Prophete, LLP ("Constangy") represents TransMedics, Inc. ("TransMedics") in connection with the data security incident described below.

Nature of the Security Incident

On April 11, 2023, TransMedics began noticing unusual activity within its network environment. After taking steps to secure the environment, TransMedics engaged an outside cybersecurity firm to conduct a forensic investigation to determine the nature of the activity and whether any TransMedics data may have been affected. That investigation revealed that a malicious actor gained access to the TransMedics network between April 6-11, 2023, and accessed and/or acquired files stored in the company's shared file folders. TransMedics reviewed the files stored in these folders in detail and confirmed on May 12, 2023 that certain individuals' personal information was included within the potentially impacted data. The information involved may include names, Social Security numbers, driver's license numbers, passport numbers, dates of birth, digital signatures, birth/marriage certificates, tax, medical or health insurance information, and work evaluation information for current and former TransMedics employees and their dependents. TransMedics is unaware of any actual or attempted misuse of this information.

Number of Maine Residents Involved

On May 25, 2023, TransMedics will be notifying five (5) Maine residents of this incident via U.S. First-Class Mail. A sample copy of the notification letter being sent to impacted individuals is included with this correspondence.

Steps Taken to Address the Incident

TransMedics has implemented additional security measures in its environment to reduce the risk of a similar incident occurring in the future. TransMedics also reported the incident to the Federal

Bureau of Investigation and is cooperating with its investigation. In addition, out of an abundance of caution, TransMedics is providing notified individuals with complimentary credit monitoring and identity protection services along with additional resources to assist them. TransMedics has also established a toll-free call center to address any questions and to help individuals resolve issues if their identity is compromised due to this incident.

Contact Information

If you have any questions or need additional information, please do not hesitate to contact me at dmcmillan@constangy.com or 718.614.8371.

Sincerely,

David McMillan of
Constangy, Brooks, Smith & Prophete, LLP

Enclosure: Sample Notification Letter

TransMedics, Inc.
Return to IDX
4145 SW Watson Ave, Suite 400
Beaverton, OR 97005

To Enroll, Please Call:
1-800-939-4170
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: <<XXXXXXXX>>

<<First Name>> << Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip Code>>

May 25, 2023

Subject: Notice of Data <<Variable Text 1>>

Dear <<First Name>> << Last Name>>:

We are writing to notify you about a recent cybersecurity incident at TransMedics that may have affected your personal information. Please read this letter carefully as it contains details about the incident and resources you can utilize to protect your information, including instructions for enrolling in complimentary credit monitoring and identity theft protection services services.

What Happened? On April 11, 2023, we began noticing unusual activity within our computer network. We activated our incident response protocols and took steps to secure our environment with the assistance of outside cybersecurity experts. The cybersecurity firm also conducted a forensic investigation to determine the nature of the activity and whether any TransMedics data may have been affected. During the course of that investigation, we learned of evidence reasonably suggesting that files containing personal information for TransMedics employees may have been accessed without authorization. The investigation has now concluded and confirmed that a malicious actor gained access to our network between April 6-11, 2023, and accessed and/or acquired files stored in the company's shared file folders. We reviewed the files stored in these folders in detail and confirmed on May 12, 2023 that your personal information was included within the potentially impacted data, which is the reason for this notification.

What Information Was Involved? Based on our investigation, we believe that the following information for current and former TransMedics employees and their dependents may have been accessed without authorization: names, Social Security numbers, driver's license numbers, passport numbers, dates of birth, digital signatures, birth/marriage certificates, tax, medical or health insurance information, and work evaluation information. Please note that we have no evidence of any actual or suspected misuse of this information. We believe any future risk to this information remains low.

What Are We Doing? Since we discovered this incident, we have taken steps to secure our environment and have enlisted a leading, independent cybersecurity firm to conduct a forensic investigation. We also reported the incident to the FBI and are cooperating in their investigation to hold the perpetrators accountable. In addition, we have implemented several technical measures in our environment to bolster TransMedics' security posture and reduce chances of a similar incident occurring again. Several additional measures are being actively considered for future implementation.

In addition, we are offering you complimentary credit monitoring and identity theft protection services through IDX – a data breach and recovery services expert. These services include: [12 months/24 months] of credit[1] and CyberScan

[1] To receive credit monitoring services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. To enroll, please call 1-800-939-4170 or visit https://app.idx.us/account-creation/protect and provide the enrollment code at the top of this page. Please note that the deadline to enroll is August 25, 2023.

What Can You Do? We encourage you to enroll in the complimentary credit protection services we are offering. With this protection, IDX can help you resolve issues if your identity is compromised. Please also review the guidance at the end of this letter which includes additional resources you may utilize to help protect your information.

For More Information: If you have questions about this matter or need assistance enrolling in the complimentary services being offered to you, please call IDX at 1-800-939-4170 from 9:00 A.M. to 9:00 P.M. Eastern Time, Monday through Friday (excluding holidays).

We take the safety and security of all TransMedics information very seriously and are pleased to offer the services described above. We will continue to invest in enhancing our cybersecurity protocols and remind all to remain vigilant to phishing campaigns.

Kind regards,

Susan Goodman

Susan Goodman | Vice President, Human Resources

TransMedics

200 Minuteman Road Suite 302
Andover, Massachusetts 01810

Steps You Can Take to Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and 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 also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Request a Copy of Your 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 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 also can contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Place a Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. 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. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at https://www.annualcreditreport.com.

Put a Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. 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 potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. 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 insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission (FTC)
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General
Bureau of Internet and Technology Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
http://www.riag.ri.gov
1-401-274-4400

Washington D.C. Attorney General
441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA and your rights pursuant to the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.