WILMERHALE

February 5, 2019

**Jason C. Chipman**

+1 202 663 6195 (t)
+1 202 663 6363 (f)
jason.chipman@wilmerhale.com

**By Federal Express**

Attorney General Gordon J. MacDonald
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Incident Notification

Dear Attorney General MacDonald:

I am writing on behalf of Abbott Laboratories to advise you of a data security incident that impacted personal information of approximately 50 residents of the State of New Hampshire.

Abbott Laboratories is a healthcare company headquartered in Illinois. On January 9, 2019, Abbott provided its third-party auditor with information about certain employee stock options and stock grants. Stock information was requested by the third-party auditor as part of the Abbott audit process. The data was loaded on the auditor's portable drive, and included fields for employee name, Social Security number, date of birth, Abbott internal employee ID, and general information about employee stock options and stock grants.

Although the drive was not intended to leave Abbott property and, by past practice, was to be deleted immediately after use by the auditor, on January 19, 2019 the auditor informed Abbott that the drive had been misplaced. Abbott immediately began an investigation into the actions of the auditor and circumstances leading to the loss of the drive, as well as to determine whether proper procedures were followed. Although we have no information suggesting that the drive was improperly accessed, it has not been recovered.

Abbott's investigation to locate the drive is ongoing. Abbott has also conducted a thorough review of the affected records to identify impacted individuals and gather their contact information. Abbott is preparing notifications about this incident that will be mailed to affected individuals on February 6, 2019. A copy of the information that will be sent to impacted individuals is also attached to this letter.

Abbott has arranged for a third party to provide identity protection services to affected individuals for 24 months. This includes access to a dedicated investigator who will help individuals recover financial losses, restore credit, and assist returning identity to its proper condition in the event of a problem. Affected individuals are also being provided with the ability to set, renew, and remove

one year fraud alerts on their credit file, as well as with credit monitoring services, a once annual credit score and credit report, and a $1 million identity theft insurance policy.

Thank you for your attention to this matter. If you have any questions or concerns, please do not hesitate to contact me.

Sincerely,

Jason C. Chipman

Encl: Sample Notice Letter

**Abbott**
Processing Center • P.O. BOX 141578 • Austin, TX 78714

00001
R903101
[redacted]

**Notice of Data Breach**

February 6, 2019

Dear [redacted],

We are writing to notify you of a data security incident that occurred at Abbott involving the potential loss of some of your personal information. We take the privacy and protection of our employees' information very seriously. We deeply regret this incident and, as described below, we are taking steps to mitigate potential harm to you as a result of this incident.

**What Happened**

On January 9, 2019, as part of a regular audit process, Abbott provided its third-party auditor with a portable drive containing information about certain employee stock options and stock grants. On January 19, 2019, the auditor informed us that the drive was misplaced. We immediately began an investigation into the actions of the auditor and circumstances leading to the loss of the drive. Although we have no information suggesting that the drive was improperly accessed, it has not been recovered, and we are notifying individuals who had some of their personal information on the drive out of an abundance of caution.

**What Information Was Involved**

The drive included fields for employee name, Social Security number, date of birth, Abbott internal employee ID (or UPI), and general information about employee stock options and stock grants.

**What We Are Doing**

Our employees' trust is a top priority for Abbott, and we deeply regret the inconvenience this may cause. Since becoming aware of this incident, Abbott and its third-party auditor have launched investigations to locate the drive as well as to determine whether proper procedures were followed. Abbott is also reassessing its own internal controls and the controls of its third-party auditor to ensure that Abbott employee data continues to be treated appropriately.

As an added precaution, we have arranged to have AllClear ID protect your identity for 24 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 24 months.

*AllClear Identity Repair*: This service is automatically available to you with no enrollment required. If a problem arises, simply call [redacted] and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

01-02-1

*AllClear Fraud Alerts with Credit Monitoring*: This service offers the ability to set, renew, and remove 1-year fraud alerts on your credit file to help protect you from credit fraud. In addition, it provides credit monitoring services, a once annual credit score and credit report, and a $1 million identity theft insurance policy. To enroll in this service, you will need to provide your personal information to AllClear ID. You may sign up online at [redacted] or by phone by calling [redacted] using the following redemption code: Redemption Code.

Please note: Following enrollment, additional steps are required by you in order to activate your phone alerts and fraud alerts, and to pull your credit score and credit file. Additional steps may also be required in order to activate your monitoring options.

**What You Can Do**

There are steps you can take to protect yourself, such as placing a freeze on your credit report or contacting the appropriate authorities if you believe you have been the victim of identity theft. The enclosed "Identity Theft Protection Tips" describes some of these steps. Of course, it is always important that you remain vigilant by reviewing your account statements and monitoring free credit reports for signs of fraud.

**For More Information**

To file a report of identity theft and to obtain more information about combating identity theft, you can contact the Federal Trade Commission at the phone number and address included in the enclosed "Identity Theft Protection Tips."

If you have further questions or concerns about this incident, please call [redacted], Monday through Saturday, 8:00 a.m. to 8:00 p.m. Central Time (excluding US holidays).

Sincerely,

Abbott Laboratories

Enclosures: (1) Identity Theft Protection Tips
(2) State Information

## Identity Theft Protection Tips

*Monitor Your Accounts*

You should remain vigilant for incidents of fraud, identity theft, and errors by regularly reviewing your account statements and monitoring free credit reports. If you discover any suspicious or unusual activity on your accounts, be sure to report it immediately to your financial institutions, as major credit card companies have rules that restrict them from requiring you to pay for fraudulent charges that are timely reported.

In addition, you are encouraged to contact the Federal Trade Commission (FTC), law enforcement, or your state attorney general to report incidents of suspected identity theft or to learn about steps you can take to protect yourself from identity theft. You can contact the FTC at:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
www.identitytheft.gov

If you find that your information has been misused, the FTC encourages you to file a complaint with the FTC and to take these additional steps, among others: (1) close the accounts that you have confirmed or believe have been tampered with or opened fraudulently; and (2) file and keep a copy of a local police report as evidence of the identity theft crime.

*Obtain Your Credit Reports*

You should also monitor your credit reports. You may periodically obtain credit reports from each nationwide consumer reporting agency. If you discover inaccurate information or a fraudulent transaction on your credit report, you have the right to request that the consumer reporting agency delete that information from your credit report file.

In addition, under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide consumer reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at https://www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf, and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also contact any of the three major consumer reporting agencies to request a copy of your credit report.

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

*Place a Fraud Alert or Security Freeze on Your Credit File*

In addition, you may obtain information from the FTC and the consumer reporting agencies about fraud alerts and security freezes. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. If you suspect you may be a victim of identity theft, you may place a fraud alert in your file by calling just one of the three nationwide consumer reporting agencies listed on the following page. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file. An initial fraud alert will last one year. An extended alert stays on your file for seven years. To place either of these alerts, a consumer reporting agency will require you to provide appropriate proof of your identity, which may include your Social Security number. If you ask for an extended alert, you will have to provide an identity theft report.

Also, you can contact the nationwide consumer reporting agencies regarding if and how you may place a security freeze on your credit report. A security freeze prohibits a consumer reporting agency from releasing information from your credit report without your prior written authorization, which makes it more difficult for unauthorized parties to open new accounts in your name. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.

You may contact the nationwide consumer reporting agencies at:

Equifax
P.O. Box 105788
Atlanta, GA 30348
(800) 525-6285
www.equifax.com

Experian
P.O. Box 9554
Allen, TX 75013
(888) 397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19016
(800) 680-7289
www.transunion.com

## State Information

**IF YOU ARE AN IOWA RESIDENT:**

You may contact local law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. You can contact the Iowa Attorney General at:

Office of the Iowa Attorney General
Hoover State Office Building
1305 E. Walnut Street
Des Moines, IA 50319
(515) 281-5926 / (888) 777-4590
www.iowaattorneygeneral.gov

**IF YOU ARE A MARYLAND RESIDENT:**

You may obtain information about avoiding identity theft from the Maryland Attorney General's Office. This office can be reached at:

Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023
www.marylandattorneygeneral.gov

**IF YOU ARE A NORTH CAROLINA RESIDENT:**

You may obtain information about preventing identity theft from the North Carolina Attorney General's Office. This office can be reached at:

North Carolina Department of Justice
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226
www.ncdoj.gov

**IF YOU ARE AN OREGON RESIDENT:**

You may report suspected identity theft to and obtain information about preventing identity theft from the Oregon Attorney General's Office. This office can be reached at:

Oregon Department of Justice
1162 Court Street NE
Salem, OR 97301-4096
(503) 378-4400
www.doj.state.or.us