DLA Piper LLP (US)
1201 North Market Street
Suite 2100
Wilmington, Delaware 19801-1147
www.dlapiper.com

Edward J. McAndrew

September 11, 2020

VIA EMAIL: doj-cpb@doj.nh.gov

The Honorable Gordon MacDonald
Consumer Protection Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Security Incident Notification

Dear Attorney General MacDonald:

We are providing notice on behalf of Eisai Inc. ("Eisai") to the New Hampshire Office of the Attorney General, pursuant to N.H. Rev. Stat. §§ 359-C:19 *et seq.*, regarding an incident involving 49 New Hampshire residents.

On or about May 15, 2020, Eisai received a user report of suspicious activity in her Eisai email account. Eisai immediately launched an investigation, with the assistance of a leading cybersecurity firm, which revealed email phishing attempts targeting a very small group of Eisai employee email accounts. The investigation also revealed suspicious login activity relating to a particular email account between May 7 and May 15, 2020. On August 10, 2020, we determined that limited personal information for 49 New Hampshire residents was contained in the email account. Our investigation revealed no evidence that any particular email message containing personal information was actually accessed by any unauthorized individual.

The email account contained the following types of personal information about the residents: Name, Tax ID Number, Driver's License Number, Passport Number, Digital or Electronic Signature, and Financial Account Number/Routing Number.

Eisai takes this incident, and information security, very seriously. Eisai takes numerous actions designed to prevent unauthorized access to our employee email accounts, including robust access and authentication controls. Eisai has secured the relevant email account and continues to monitor for suspicious activity. Eisai continues to enhance its identity, authentication and remote access controls, and educate its workforce about cybersecurity issues.

In an abundance of caution, Eisai is notifying potentially affected individuals and providing them with access to 24 months of Experian IdentityWorks^{SM} identity protection services, which includes: Experian credit report at enrollment, credit monitoring, identity restoration services, extended services, and a $1 million identity theft insurance policy.

DLA PIPER

VIA FIRST CLASS MAIL

Eisai mailed written notification to the affected residents on September 10, 2020. A sample notification letter is enclosed.

If you should have any questions or if we can provide further assistance to the New Hampshire residents affected by this incident, please feel free to contact me at (302) 468-5685 or ed.mcandrew@dlapiper.com.

Respectfully submitted,

DLA Piper LLP (US)

Edward J. McAndrew
An Attorney for Eisai Inc.

Enclosure

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

September 10, 2020

F7735-L02-0000002 T00001 **********OEL LINE
SAMPLE A SAMPLE - L02
APT #123
123 ANY ST
ANYTOWN, US 12345-6789

RE: Notice of Data Security Incident

Dear Sample A Sample:

We write to share important information with you about a data security incident that may have impacted your personal information. The protection of confidential information is among Eisai's highest priorities. We sincerely apologize and we take the security of your personal information very seriously.

We want to begin by emphasizing that we have no evidence that your personal information has been accessed without authorization or compromised. In an abundance of caution, we are providing this notice to you so you know what we are doing and the steps you can take to protect your information should you feel it is appropriate to do so.

What Happened? We have conducted an investigation, with the assistance of a leading cybersecurity firm, into email phishing attempts targeting a very small group of Eisai employees. On August 10, 2020, we determined that your personal information was contained in an email account that appears to have been accessed by an unauthorized individual. The dates of potential unauthorized access was between May 7 and May 15, 2020. Although the employee email account itself appears to have been accessed by an unauthorized individual, our investigation revealed no evidence that any email message containing your personal information was actually accessed by an unauthorized individual.

What Information Was Involved? The types of personal information contained in the email account varied by individual. In general, a limited number of emails contained in the email account may have included one or more of the following types of personal information: Name, Tax ID Number, Driver's License Number, Passport Number, Digital or Electronic Signature, and financial account/routing number.

What We Are Doing. We take this incident, and information security, very seriously. We take numerous actions designed to prevent unauthorized access to our employee email accounts. Upon learning of the phishing activity, we immediately launched an investigation with the assistance of leading cybersecurity experts. We have secured the relevant email account and we continue to monitor for suspicious activity. We are continuing to enhance our identity, authentication and remote access controls, and to educate our workforce about cybersecurity issues.

What You Can Do. As an added precaution, we have arranged to have Experian IdentityWorks℠ protect your identity for twenty-four months at no cost to you. The following identity protection services start as of the date of this letter above, but you must enroll in the service by December 31st, 2020. A description of the service and details for activating your complimentary account are below.

24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

We encourage you to activate your complimentary Experian IdentityWorks℠ membership today. This product provides you with superior identity detection and resolution of identity theft.

To start monitoring your personal information please follow the steps below:

- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/credit
- Provide your **activation code: ABCDEFGHI**
- Ensure that you **enroll by: December 31st, 2020**

Once you enroll in Experian IdentityWorks, you will have access to the following features:

- **Experian credit report at signup:** See what information is associated with your credit file.
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration**: Identity Restoration agents 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.
- **$1 Million Identity Theft Insurance:** Provides coverage for certain costs and unauthorized electronic fund transfers.

A credit card is **not** required for enrollment in Experian IdentityWorks, and there is no cost to you for this complimentary 24-month service.

EXPERIAN IDENTITY RESTORATION

If you believe there has been fraudulent use of your information as a result of this incident, please contact an Experian agent at **1-877-890-9332** and provide your engagement number **DB22472** as proof of eligibility for the identity restoration services by Experian.

If 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 this service is available to you for twenty-four months from September 10, 2020, but you must enroll by December 31st, 2020.

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.

The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.
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 **1-877-890-9332** by **December 31st, 2020**. Be prepared to provide engagement number **DB22472** as proof of eligibility for the identity restoration services by Experian.

For More Information. We sincerely regret any concern this incident may cause you. If you have questions or concerns that are not addressed in this notice letter, please contact me at 201-746-2913.

Sincerely,

Jaideep Singh
Director, IT-Security

0000002

F7735-L02

Steps You Can Take to Protect Against Identity Theft and Fraud

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised 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. Under federal law, you cannot be charged to place, lift or remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. To find out more on how to place a security freeze, you can use the following contact information:

Equifax	Experian Security Freeze	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094
800-349-9960	888-397-3742	888-909-8872

Websites:
www.equifax.com/personal/credit-report-services/credit-freeze
www.experian.com/freeze/center.html
www.transunion.com/credit-freeze
To request a security freeze, you will need to provide some or all of the following information to the credit reporting agency, depending on whether you do so online, by phone, or by mail.:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of Birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years;

5. Proof of current address, such as a current utility bill, telephone bill, rental agreement, or deed;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. Social Security Card, pay stud, or W2;
8. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit report, based upon the method of your request. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password (or both) that can be used by you to authorize the removal or lifting of the security freeze. It is important to maintain this PIN/password in a secure place, as you will need it to lift or remove the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (including name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report. You may also temporarily lift a security freeze for a specified period of time rather than for a specific entity or individual, using the same contact information above. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for request made by mail) after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the 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 credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center
Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.