EDWARDS WILDMAN

EDWARDS WILDMAN PALMER LLP
20 CHURCH STREET
HARTFORD, CT 06103
+1 860 525 5065 main +1 860 527 4198 fax
edwardswildman.com

Theodore P. Augustinos
+1 860 541 7710
fax +1 888 325 9082
taugustinos@edwardswildman.com

Via Federal Express

July 9, 2012

Attorney General Michael A. Delaney
New Hampshire Department of Justice
33 Capitol Street
Concord, NH 03301

Re: Neurocare, Inc.
Notification of Potential Security Breach under N.H. Rev. Stat. § 359-C.20

Dear Attorney General Delaney:

On behalf of our client, Neurocare, Inc., we write to advise you of an incident involving an unauthorized intrusion by one or more unidentified individuals into Neurocare's computer systems, resulting in the potential compromise of the personal information of Neurocare employees resident in New Hampshire. The incident occurred remotely through a malware attack on a Neurocare CPU located in Newton, Massachusetts. The malware attack appears to have compromised Neurocare's credentials for accessing its account at its third party payroll processor, resulting in unauthorized access into Neurocare's payroll system on or about June 26, 2012. Based on Neurocare's investigation, which is described below, the intrusion potentially exposed certain personal information of approximately 136 Neurocare employees and/ or former employees, six of whom are New Hampshire residents, to unauthorized access.

Learning About the Incident. On June 26, 2012, Neurocare was notified by its payroll processing vendor that it had received instructions from Neurocare to re-route a suspiciously large number of employee automatic payroll deposits. As Neurocare had not provided such instructions, the account was immediately disabled by the payroll processor.

Upon learning of the incident, Neurocare immediately took the following actions: (1) notified local law enforcement; (2) changed Neurocare passwords to its systems, including its payroll systems; (3) advised Neurocare employees that it was investigating an incident that may have involved the compromise of certain information and recommended that employees monitor their direct deposit bank account for suspicious activity; (4) scanned Neurocare's computer systems for malware and intrusions; (5) engaged special outside counsel to provide legal advice as to Neurocare's legal obligations; (6) engaged a forensic investigation firm to conduct an investigation of the incident and to recommend further security enhancements; and (7) committed to notify and offer solutions to affected individuals.

The payroll processor would not provide Neurocare with the results of its investigation, which they advised would be provided to the United States Secret Service, but they provided Neurocare with an Employee Changes Report indicating that 17 employee accounts had unauthorized changes made to bank accounts set up for automatic deposit. These changes were caught and reversed before payroll was transacted. The payroll processor subsequently provided Neurocare with the two unauthorized IP addresses that were used in the attack. Neurocare subsequently learned that two additional Neurocare employee files had been viewed, bringing the total to 19. The payroll processor advised that they had no further evidence that accounts were accessed but also could not rule out that the information of other Neurocare employees may have been accessed.

Investigating the Disclosure. The forensic investigators determined that a Neurocare computer used to process payroll had been infected by malware. The malware apparently compromised Neurocare's login credentials providing access to its payroll entry system, and provided unauthorized access to the payroll processor, exposing the following types of information of Neurocare employees: name, Social Security number, date of birth, tax deductions, bank account information contained on a personal check, and home address.

Although the investigation determined that the personal information of 19 employees had been accessed, the compromise of the login credentials could have also exposed the information of all other Neurocare employees to unauthorized access.

The forensic investigation found no indication that any personal health information on the Neurocare system was a target of the intrusion, or that any such information was accessed or acquired as a consequence of the breach.

At this time, Neurocare, Inc. has no knowledge that the personal information of any Neurocare employee has been misused as a consequence of the breach, other than the failed attempts to redirect payroll described above. Neurocare is also unaware of any reported instance of identity theft related to this incident.

Communicating with Affected Individuals. To enable affected individuals to take immediate steps to protect themselves from possible identity theft or other monetary damage, Neurocare will promptly notify each of them of the incident by sending notices via first-class mail on July 11, 2012. The notification materials are enclosed with this letter as Exhibit A.

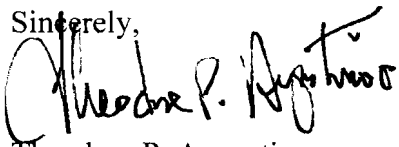
Services to Affected Individuals. The notification materials will describe the various services Neurocare has made available, free of charge, to affected individuals through Experian. Neurocare has instructed Experian to provide affected individuals access for one year to its ProtectMyID Elite Program, providing identity theft detection, protection and resolution services, and to its ExtendCARE Fraud Resolution program, providing long-term fraud

resolution services. Neurocare believes the services offered to affected individuals will help them immediately respond to any threats of identity theft or other misuse of their data as a result of this isolated incident.

Efforts to Deter Future Breach. Neurocare has taken and is in the process of implementing several important steps to improve the level of its data security in response to this incident, including the following: (1) increasing the profile of data security issues at all levels; (2) installation of a separate CPU dedicated to payroll processing only; (3) modification of firewall settings-lockout period; (4) increased restriction of firewall administration account access; and (5) enhancement of intrusion detection and firewalls.

We trust that this letter and its enclosure provide you with all of the information required to assess this incident and Neurocare's response. Please let us know if you have any questions or if we may be of further assistance.

Sincerely,



Theodore P. Augustinos

Enclosure

EXHIBIT A

[Neurocare, Inc. Letterhead]

Urgent Message
Please Open Immediately

[Date]

[Name]
[Address]

Dear [Name]:

Regrettably, on June 26, 2012, there was an unauthorized intrusion into our computer system. This resulted in the potential compromise of the security of your personal information including your Social Security number, address, date of birth, bank account information contained on a personal check, home address, salary information and tax elections. Our detailed investigation revealed no evidence that your information was subject to unauthorized acquisition. However, we cannot rule out the possibility that your information was accessed.

We are writing to inform you of the data intrusion incident and the steps we have been taking to help safeguard your personal information. We have engaged an independent forensic investigation firm to determine the scope of the incident, and to recommend enhancements to our security.

In addition, to provide you with an additional measure of security and assistance, we are offering a complimentary one-year membership in Experian's ProtectMyID™ Elite. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on identification and resolution of identity theft. To activate the ProtectMyID service, please follow the instructions below:

1. Ensure that you enroll by October 31, 2012.
2. Visit the ProtectMyID Web Site: www.protectmyid.com/enroll or call 877-441-6943 to enroll.
3. Provide Your Activation Code: [code]

Once your ProtectMyID membership is activated, your credit report will be monitored daily for 50 leading indicators of identity theft. You will receive timely Surveillance Alerts™ from ProtectMyID on any key changes in your credit report, a change of address, or if an Internet Scan detects that your information may have been found in an online forum where compromised credentials are traded or sold.

ProtectMyID provides you with identity protection that will help detect, protect and resolve potential identity theft. In the case that identity theft is detected, ProtectMyID will assign a dedicated U.S.-based Identity Theft Resolution Agent who will walk you through the process of fraud resolution from start to finish.

We realize that identity theft can happen months and even years after a data breach. To offer added protection, you will receive ExtendCARE™, which provides you with the same level of Fraud Resolution support after your ProtectMyID membership has expired.

Your complimentary 12-month ProtectMyID membership includes the following:

- **Credit Report:** A free copy of your Experian credit report
- **Surveillance Alerts**
  - **Daily 3 Bureau Credit Monitoring:** Alerts you of suspicious activity including new inquiries, newly opened accounts, delinquencies, or medical collections found on your Experian, Equifax, and TransUnion credit reports
  - **Internet Scan:** Alerts you if your Social Security number or Credit and/or Debit Card numbers are found on sites where compromised data is found, traded or sold.
  - **Change of Address:** Alerts you of any changes in your mailing address.
- **Identity Theft Resolution:** If you have been a victim of identity theft, you will be assigned a dedicated, U.S.-based Experian Identity Theft Resolution Agent who will walk you through the fraud resolution process, from start to finish.
- **ExtendCARE:** Full access to the same personalized assistance from a trained Fraud Resolution Agent after your initial ProtectMyID membership expires.
- **Lost Wallet Protection:** If you misplace or have your wallet stolen, an agent will help you cancel your credit, debit and medical insurance cards.
- **$1 Million Identity Theft Insurance:**[1] As a ProtectMyID member, you are immediately covered by a $1 Million insurance policy that can help you cover certain costs, including lost wages, private investigator fees, and unauthorized electronic fund transfers.

Once your enrollment in ProtectMyID is complete, you should carefully review your credit report for inaccurate or suspicious items. Enclosed is an insert containing certain information required to be provided to residents of certain states in the event of a data breach.

If you have any questions about this incident or the ProtectMyID services, please contact Experian's customer care team at 877-441-6943. If you would like to speak with someone at Neurocare, Inc. to clarify or discuss the authenticity of this letter, please contact us at 617-581-6407.

We are committed to protecting your privacy and to communicating with you promptly if it is compromised. We regret any inconvenience or concern that the data intrusion may

[1] This identity theft insurance is underwritten by insurance company subsidiaries or affiliates of Chartis, Inc. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

have caused. We believe it is important to inform you of any potential risk. We are providing you with quality professional assistance in handling matters that may arise as a result of this incident, even though we have no evidence that your personal information has actually been accessed or misused. Protecting your privacy is a key priority for us. We will maintain vigilance and will take steps as needed to continue to improve our privacy and data security safeguards.

Sincerely,

John M. Leteria
Chief Executive Officer