ADVANCED DATA PROCESSING, INC.

November 28, 2012

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

Dear Attorney General Delaney:

On behalf of Advanced Data Processing, Inc. and its subsidiaries (the "Company") and those Company clients listed on the attached schedule, we are writing to notify you of a recent incident involving the personal information of certain residents of your state. The details of this incident and related information are provided below.

The Company performs billing services for municipal emergency medical services and is a covered entity under the federal Health Insurance Portability and Accountability Act ("HIPAA"). On October 1, 2012, The Company was notified by the Tampa, Florida Police Department that they had obtained copies of the Company's records from an individual engaged in a scheme to file false tax returns. Upon further investigation, we learned that a Company employee was a participant in this scheme and we terminated the employee. The types of information improperly accessed included names, social security numbers and dates of birth. No clinical medical information was accessed. Federal and local law enforcement agencies continue to be involved in this matter and we have cooperated fully with them. The Company has also conducted its own investigation and risk assessment using internal resources and outside experts.

As of this date, we believe that 2 residents of your state are affected by this incident (which figure includes, out of an abundance of caution, individuals for whom we cannot rule out that their information was not improperly accessed and disclosed). The Company has undertaken notice in compliance with the applicable HIPAA breach notification rules. The attached forms of notice were previously sent or will be sent by regular mail on or about November 29, 2012 (a) in the case of the notice at Exhibit A, to those residents of your state whose personal information we know was improperly accessed, and (b) in the case of the notice at Exhibit B, to those residents of your state for whom we cannot rule out that their information was not improperly accessed and disclosed. Separately, we have also provided (or are in the process of providing) notice of this incident to the Secretary of Health and Human Services and the three major national credit bureaus.

To minimize the recurrence and risk of similar incidents, among other things, the Company is making its employees aware of this incident and the consequences to the individual involved and reminding its employees of the importance of maintaining at all times the security and confidentiality of individual records. The Company also engaged an outside consulting firm, ID Experts, Inc., to assist the Company with assessing the risks associated with the present incident.

Please be assured that the Company takes seriously its responsibility to protect sensitive account information. If your office requires any further information in this matter, please contact the undersigned at the above address or by telephone at 954-308-8702.

Sincerely,

Gregg Bloom,
Vice President and Chief Compliance Officer

Schedule to Advanced Data Processing, Inc. Notice Letter to State of New Hampshire

This notice is also being provided on behalf of the following agencies that are clients of the Company:

City of Atlanta EMS, Georgia
City of Gloucester, Massachusetts

EXHIBIT A

ADPI Letterhead Reference Number: < >

November x, 2012

This notice is sent to you on behalf of Advanced Data Processing, Inc. (the "Company") and _____ (the "Ambulance Agency") to alert you to an important matter. The Company manages billing for ambulance agencies. We learned on October 1, 2012 that an employee of the Company illegally accessed and disclosed certain patient account information in connection with a scheme to file false federal tax returns. Accessed account information included name, date of birth, Social Security number and record identifier. No medical information was accessed.

Our investigation of this matter has found that your account information may have been disclosed. It is not known whether your information was actually misused. Because we cannot rule out that your information may have been actually misused, out of an abundance of caution, we are providing you with this notice.

The employee has been apprehended by authorities, was immediately terminated by the Company and no longer has access to our system. To help minimize the risk of future data breaches, the Company is making its employees aware of this incident and the consequences to the individual involved and reminding its employees of the importance of maintaining the security and confidentiality of individual records.

If you have reason to believe that your information is being misused, you should contact local law enforcement (including your State Attorney General's Office) and file a police report. Creditors may want a copy of the police report to absolve you of any fraudulent debts. In addition, if you believe a tax return has been illegally filed using your information you should contact your local IRS Service Center or call the IRS at 1-800-908-4490. You may obtain additional information from the IRS website www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft.

We advise you to remain vigilant and monitor your credit reports. Even if you do not find any suspicious activity, you should continue to check your credit reports periodically. To help you detect possible misuse of your personal information and provide you with identity protection services, we are offering a complimentary one year membership of Experian's® ProtectMyID® Alert. You have 90 days to activate this membership, which will then continue for 1 year. Visit www.protectmyid.com/redeem or call 1-877-371-7902 to enroll and simply provide your Individual Activation Code: [code]

You also may wish to consider placing a fraud alert or security freeze on your credit report. A fraud alert requires creditors to contact you before they open any new accounts or change your existing accounts. A security freeze prohibits a credit reporting agency from releasing any information from your credit report without your written authorization. Contact information for the three major national credit bureaus is available on the _____ website along with additional information for residents of specific states, which may be of interest to you, even if you are not a resident.

You may call 1-XXX-XXXX X a.m. to X p.m. Eastern Monday through Friday, if you have any questions regarding this matter.

Please be assured we take our responsibility to protect sensitive account information seriously. Unfortunately, illegal activity conducted from within by an employee who chooses to engage in criminal activity cannot always be prevented. We apologize for any inconvenience this incident may cause you.

EXHIBIT B

ADPI Letterhead

Reference Number: < >

November x, 2012

This notice is sent to you on behalf of Advanced Data Processing, Inc. (the "Company") and _____ (the "Ambulance Agency") to alert you to an important matter. The Company manages billing for ambulance agencies. We learned on October 1, 2012 that an employee of the Company illegally accessed and disclosed certain patient account information in connection with a scheme to file false federal tax returns. Accessed account information included name, date of birth, Social Security number and record identifier. No medical information was accessed.

Our investigation of this matter has found that your account information may have been disclosed. It is not known whether your information was actually misused. Because we cannot rule out that your information may have been actually misused, out of an abundance of caution, we are providing you with this notice.

The employee has been apprehended by authorities, was immediately terminated by the Company and no longer has access to our system. To help minimize the risk of future data breaches, the Company is making its employees aware of this incident and the consequences to the individual involved and reminding its employees of the importance of maintaining the security and confidentiality of individual records.

If you have reason to believe that your information is being misused, you should contact local law enforcement (including your State Attorney General's Office) and file a police report. Creditors may want a copy of the police report to absolve you of any fraudulent debts. In addition, if you believe a tax return has been illegally filed using your information you should contact your local IRS Service Center or call the IRS at 1-800-908-4490. You may obtain additional information from the IRS website www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft.

We advise you to remain vigilant and monitor your credit reports periodically. The Fair Credit Reporting Act requires each of the nationwide consumer reporting companies — Equifax, Experian, and TransUnion — to provide you with a free copy of your credit report, at your request, once every 12 months. To order, visit annualcreditreport.com or call 1-877-322-8228. You may also choose to enroll in a free credit monitoring service.

You also may wish to consider placing a fraud alert or security freeze on your credit report. A fraud alert requires creditors to contact you before they open any new accounts or change your existing accounts. A security freeze prohibits a credit reporting agency from releasing any information from your credit report without your written authorization. Contact information for the three major national credit bureaus is available on the _____ website along with additional information for residents of specific states, which may be of interest to you, even if you are not a resident.

You may call 1-XXX-XXXX X a.m. to X p.m. Eastern Monday through Friday, if you have any questions regarding this matter.

Please be assured we take our responsibility to protect sensitive account information seriously. Unfortunately, illegal activity conducted from within by an employee who chooses to engage in criminal activity cannot always be prevented. We apologize for any inconvenience this incident may cause you.