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

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

Berkeley FD, California
City of Corona FD, California
El Centro FD, California
Los Angeles FD, California

EXHIBIT A (For patients whose data the Company has confirmed was improperly accessed)

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 (For patients whose data the Company cannot rule out was not improperly accessed)

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.