



To Enroll, Please Call:
1-866-599-2071
Or Visit:
my.idmonitoringservice.com
Membership Number: <<Member ID>>

<<Date>> (Format: Month Day, Year)

<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>> <<Suffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<ZipCode>>

Subject: Notice of Data Security Incident

Dear <<MemberFirstName>> <<MemberLastName>>,

I am writing to inform you of a potential data security incident that may have involved your personal information. Acadiana Computer Systems (“ACS”) performs electronic medical billing services for healthcare providers, including <<ClientDef1(Provider Name)>>. ACS takes the privacy and security of its client information very seriously. This is why I am notifying you of a recent incident, offering you identity monitoring services, and providing you information about steps that you can take to help protect your personal information.

What Happened? ACS learned on July 6, 2018 that an employee email account had been accessed without authorization. Upon learning of the incident, ACS immediately disabled access to the account, and began an investigation to determine what happened and whether patient information had been acquired without authorization. ACS also reported the matter to the FBI. The investigation revealed that your personal information may have been involved in the incident. At this time, we are not aware of the misuse of any of your information.

What Information Was Involved? The involved information may have included your name and treatment billing information. Your Social Security number was not involved in this incident.

What Are We Doing? As soon as ACS discovered the incident, we took the steps described above. In addition, ACS is providing you with information about steps you can take to help protect your personal information and is offering you identity monitoring services through Kroll for twelve (12) months at no cost to you. Finally, ACS has taken steps to enhance the security of all client information in its possession, in order to prevent similar incidents from occurring in the future.

What You Can Do: You can follow the recommendations included with this letter to protect your personal information. In addition, while we are not aware of the misuse of any of your information, to help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Web Watcher, Fraud Consultation, and Identity Theft Restoration. Additional information describing your services is included with this letter.

Visit my.idmonitoringservice.com to activate and take advantage of your identity monitoring services.

*You have until **December 14, 2018** to activate your identity monitoring services.*

Membership Number: <<Member ID>>

For More Information: Further information about how to protect your personal information is on the following pages. If you have questions or need assistance, please call 1-866-599-2071 Monday through Friday, from 8:00 a.m. to 5:00 p.m. Central Time.

Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in black ink that reads "Jaime Hebert". The signature is written in a cursive, slightly slanted style.

Jaime Hebert, CHP
HIPAA Privacy & Information Security Officer
Acadiana Computer Systems



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services¹ from Kroll:

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

¹ Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari.

Steps You Can Take to Further Protect Your Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>. You also can contact one of the following three national credit reporting agencies:

TransUnion	Experian	Equifax	Free Annual Report
P.O. Box 1000 Chester, PA 19016 1-877-322-8228 www.transunion.com	P.O. Box 9532 Allen, TX 75013 1-888-397-3742 www.experian.com	P.O. Box 105851 Atlanta, GA 30348 1-800-525-6285 www.equifax.com	P.O. Box 105281 Atlanta, GA 30348 1-877-322-8228 annualcreditreport.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: In some U.S. states, you have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. If you request a security freeze from a consumer reporting agency there may be a fee up to \$10 to place, lift or remove the security freeze. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission	Maryland	North Carolina	Alabama
600 Pennsylvania Ave, NW Washington, DC 20580 consumer.ftc.gov , and www.ftc.gov/idtheft 1-877-438-4338	Attorney General 200 St. Paul Place Baltimore, MD 21202 oag.state.md.us 1-888-743-0023	Attorney General 9001 Mail Service Center Raleigh, NC 27699 ncdoj.gov 1-877-566-7226	Attorney General P.O. Box 300152 Montgomery, AL 36130-0152 ago.alabama.gov 1-800-392-5658

You also have certain rights under the Fair Credit Reporting Act (FCRA), including: to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information, as well as others. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf