San Mateo Medical Center
A County System of Healthcare
Processing Center ● P.O. BOX 141578 ● Austin, TX 78714

00001
ACD1234
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

May 18, 2018

Subject: NOTICE OF DATA BREACH

Dear John Sample:

What Happened?

We regret to inform you that our practice has discovered a breach of your personal health information. We became aware of this breach on December 21, 2017. A security event occurred at one of our third-party technology providers. Unfortunately, some of your personal information was part of the compromise.

The technology provider provides the San Mateo Medical Center (SMMC) with medical record transcription services. SMMC recently received notice from the technology provider that an unauthorized party had accessed certain patient reports that the technology provider enables SMMC to create to help us provide you with the best service possible. The technology provider retained CrowdStrike, a leading cybersecurity firm to conduct an investigation. The investigation determined that the unauthorized party accessed patient information between November 20, 2017 and December 9, 2017. Promptly following discovering the event, the technology provider took the affected system offline.

The technology provider concluded that there is a low risk your information was compromised. The unauthorized individual did not appear to use, sell, or otherwise transfer the information.

What Information Was Involved?

The reports accessed by the unauthorized party may have included patient name, patient date of birth, patient age, patient sex, patient social security number, patient medical record number, patient account number, patient medical transcription text, and patient date of service.

What We Are Doing:

We are working with the technology provider to address this issue. The technology provider also notified law enforcement about the event. As an added precaution, we have arranged to have AllClear ID protect your identity for 24 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 24 months.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-803-1476 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Fraud Alerts with Credit Monitoring: This service offers the ability to set, renew, and remove 90-day fraud alerts on your credit file to help protect you from credit fraud. In addition, it provides credit monitoring services, a once annual credit score and credit report and a $1 million identity theft insurance policy. For a child under 18 years old, AllClear ID ChildScan identifies acts of fraud against children by searching thousands of public databases for use of your child's information. To enroll in this service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 1-855-803-1476 using the following redemption code: Redemption Code.

Please note: Following enrollment, additional steps are required by you in order to activate your phone alerts and fraud alerts, and to pull your credit score and credit file. Additional steps may be required in order to activate all of your monitoring options.

What You Can Do:
Keep a copy of this notice for your records in case of future problems with your medical records. We also recommend that you regularly review the explanation of benefits (EOB) statement that you receive from your health insurance plan.

If you see any service that you believe you did not receive, please contact the health insurance plan at the number on the statement. If you do not receive regular explanation of benefits statements, contact your provider or plan and ask them to send such statements following the provision of services provided in your name or under your plan number.

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. Please review the enclosure "Breach Help" for information on how to obtain a credit report, a credit freeze, fraud alerts, and additional information about identity theft protection.

For More Information:
For information about your medical privacy rights, you may visit the website of the California Department of Justice, Privacy Enforcement and Protection, at www.privacy.ca.gov. For information about the services being offered, you may also contact AllClear ID at 1-855-803-1476, Monday through Saturday, 8:00 a.m. – 8:00 p.m. Central Time.

Agency Contact:
Please do not hesitate to contact Gabriela Behn, Privacy and Corporate Compliance Officer, with any questions about this incident or if you need additional information on what you should do as a result of the breach, at 1-650-573-2329.

Sincerely,

Gabriela Behn
HIPAA and Compliance Manager

Breach Help

Consumer Tips from the California Attorney General

Consumer Information Sheet 17 • October 2014

You get a letter from a company, a government agency, a university, a hospital or other organization. The letter says your personal information may have been involved in a data breach. Or maybe you learn about a breach from a news report or company web site. Either way, a breach notice does not mean that you are a victim of identity theft or other harm, but you could be at risk.

The breach notice should tell you what specific types of personal information were involved. It may also tell you what the organization is doing in response. There are steps you can take to protect yourself. What to do depends on the type of personal information involved in the breach.

Note that credit monitoring, which is often offered by breached companies, alerts you *after* someone has applied for or opened new credit in your name. Credit monitoring can be helpful in the case of a Social Security number breach. It does not alert you to fraudulent activity on your existing credit or debit card account.

Credit or Debit Card Number

The breach notice should tell you when and where the breach occurred. If you used your credit or debit card at the location during the given time, you can take steps to protect yourself.

Credit Card

1. Monitor your credit card account for suspicious transactions and report any to the card-issuing bank (or American Express or Discover). Ask the bank for online monitoring and alerts on the card account. This will give you early warning of any fraudulent transactions.

2. Consider cancelling your credit card if you see fraudulent transactions on it following the breach. You can dispute fraudulent transactions on your credit card statement, and deduct them from the total due. Your liability for fraudulent transactions is limited to $50 when you report them, and most banks have a zero-liability policy.[1]

3. If you do cancel your credit card, remember to contact any companies to which you make automatic payments on the card. Give them your new account number if you wish to transfer the payments.

Debit Card

1. Monitor your debit card account for suspicious transactions and report any to the card issuer. Ask the bank for online monitoring and alerts on the card account. This will give you early warning of any fraudulent transactions.

2. Report any unauthorized transactions to your bank immediately to avoid liability. Your liability for fraudulent transactions is limited to $50 if you report them within two days. Your bank may have a zero liability policy. But as time passes, your liability increases, up to the full amount of the transaction if you fail to report it within 60 days of its appearance on your bank statement.[2]

3. Consider cancelling your debit card. The card is connected to your bank account. Cancelling it is the safest way to protect yourself from the possibility of a stolen account number being used to withdraw money from your bank account. Even though it would likely be restored, you would not have access to the stolen money until after your bank has completed an investigation.

Social Security Number

Here's what to do if the breach notice letter says your Social Security number was involved.

1. Contact the three credit bureaus. You can report the potential identity theft to all three of the major credit bureaus by calling any one of the toll-free fraud numbers below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three bureaus. You will also be sent instructions on how to get a free copy of your report from each of the credit bureaus.

Experian	1-888-397-3742
Equifax	1-800-525-6285
TransUnion	1-800-680-7289

2. What it means to put a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that there may be fraud on the account. This alerts the merchant to take steps to verify the identity of the applicant. A fraud alert lasts 90 days and can be renewed. For information on a stronger protection, a security freeze, see ***How to Freeze Your Credit Files*** at *www.oag.ca.gov/privacy/info-sheets.*

3. Review your credit reports. Look through each one carefully. Look for accounts you don't recognize, especially accounts opened recently. Look in the inquiries section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store names. The credit bureau will be able to tell you when that is the case. You may find some inquiries identified as "promotional." These occur when a company has obtained your name and address from a credit bureau to send you an offer of credit. Promotional inquiries are not signs of fraud. (You are automatically removed from lists to receive unsolicited offers of this kind when you place a fraud alert.) Also, as a general precaution, look in the personal information section for any address listed for you where you've never lived.

4. If you find items you don't understand on your report, call the credit bureau at the number on the report. Credit bureau staff will review your report with you. If the information can't be explained, then you will need to contact the creditors involved and report the crime to your local police or sheriff's office.

Password and User ID

In the case of an online account password breach, you may receive a notice by email or when you go to the log-on page for your account. Here are steps to take if you learn that your password and user ID or email address, or perhaps your security question and answer, were compromised.

1. Change your password for the affected account. If you find that you are locked out of your account, contact the company's customer service or security department.

2. If you use the same password for other accounts, change them too.

3. If a security question and answer was involved, change it. Don't use questions based on information that is publicly available, such as your mother's maiden name, your pet's name or the name of your high school.

4. Use different passwords for your online accounts. This is especially important for accounts that contain sensitive information, such as your medical or financial information. Consider accounts at online merchants where you may have your credit card number stored in the account.

5. Create strong passwords. Longer is better—at least ten characters long and a mix of uppercase and lowercase letters, numerals, punctuation marks, and symbols. Don't use words found in a dictionary. You can base passwords on a phrase, song or book title.

   Example: "I love tropical sunsets" becomes 1luvtrop1calSuns3ts!

6. A password manager or password "safe" can help you create and manage many strong passwords. These software programs can run on your computer, your phone and other portable devices. You only have to remember one password (or passphrase) to open the safe. The Electronic Frontier Foundation (*www.eff.org*) lists some free versions and computer magazines offer product reviews.

Bank Information

If the breach notice says your checking account number, on a check for example, was breached, here's what to do.

1. Call the bank, tell them about the breach and tell them you want to close your account. Find out what checks are outstanding. You may want to wait until they have cleared before closing the account. (Or you could write to each recipient, tell them about the breach, ask them not to process the old check and enclose a new check on your new account.)

2. Open a new bank account. Tell the bank you want to use a new password for access to your new account. Do not use your mother's maiden name or the last four digits of your Social Security number. Ask your bank to notify the check verification company it uses that the old account was closed.

Driver's License Number

If the breach notice says your driver's license or California identification card number was involved, and you suspect that you are a victim of identity theft, contact DMV's Driver License Fraud and Analysis Unit (DLFAU) by telephone at 1 866-658-5758 or by email at *dlfraud@dmv.ca.gov*. Do not include personal information on your e-mail.

Medical or Health Insurance Information

If the breach notice says your health insurance or health plan number was involved, here's what you can do to protect yourself against possible medical identity theft. A breach that involves other medical information, but not your insurance or plan number, does not generally pose a risk of medical identity theft.

1. If the letter says your Social Security number was involved, see section on Social Security number breaches. Also contact your insurer or health plan, as in number 2 below.

2. If the letter says your health insurance or health plan number was involved, contact

your insurer or plan. Tell them about the breach and ask them to note the breach in their records and to flag your account number.

3. Closely watch the Explanation of Benefits statements for any questionable items. An Explanation of Benefits statement comes in the mail, often marked "This is not a bill." It lists the medical services received by you or anyone covered by your plan. If you see a service that you did not receive, follow up on it with your insurer or plan. For more on medical identity theft, see ***First Aid for Medical Identity Theft: Tips for Consumers***, at *www.oag.ca.gov/privacy/info-sheets*.

For more details on what to do if you suspect that your information is being used to commit identity theft, see the ***Identity Theft Victim Checklist*** at *www.oag.ca.gov/idtheft/information-sheets.*

NOTES

[1] Truth in Lending Act, 14 U.S. Code sec. 1601 and following.

[2] Electronic Funds Transfer Act, 15 U.S. Code sec. 1693 and following.