Moorpark Office
2400 Moorpark Ave. Suite #300
San Jose, CA 95128

[Patient Name]
[Address Line 1]
[City, State, Zip]

Dear [Patient]:

We are sending this letter to you as part of the Asian Americans for Community Involvement's ("AACI") commitment to patient privacy. We take patient privacy very seriously, and it is important to us that you are made fully aware of a potential privacy issue. We have learned that your personal information may have been comprised. This notice explains what happened, the measures we have taken in response, the additional measures that will be taken in the future, and the steps you can take for further protection.

What Happened?

From 11/08/2022 to the present, a company named OCHIN, Inc. ("OCHIN"), has provided AACI with software and support for an electronic medical records platform named Epic Software. At the same time, OCHIN contracted with a third company, Trizetto Provider Solutions ("TPS"), to provide revenue management services to numerous healthcare providers (including AACI) that were customers of OCHIN.

TPS operates a web portal that healthcare providers can use to access TPS's services. TPS's web portal contains protected health information regarding many individual patients.

On December 9, 2025, TPS informed OCHIN that TPS had experienced a data breach involving TPS's web portal.

On December 10, 2025, OCHIN informed AACI that TPS had experienced a data breach. OCHIN provided AACI with no details. OCHIN did not confirm whether or not any patients of AACI were impacted.

On December 11, 2025, OCHIN provided AACI with the following information:

> On October 2, 2025, TriZetto became aware of suspicious activity within their web portal that health care provider customers use to access TriZetto systems. The web portal also allows health care provider customers to query their historical records related to TriZetto services.
>
> Upon discovering the incident, TriZetto launched an investigation and took steps to mitigate the issue. TriZetto engaged Mandiant, an external cybersecurity expert, and with their help, reviewed the security of the affected web portal application and eliminated the threat to the environment.
>
> Analysis born out of their investigation revealed that, from November 2024 to October 2025, an unauthorized actor had access to certain historical eligibility transaction reports stored on TriZetto's system. There is no evidence of activity within the TriZetto environments by the unauthorized actor since October 2, 2025, and there is no evidence that information was downloaded. TriZetto has reported that: (1) The affected reports contain information about health insurance eligibility transactions, including certain protected health information of patients

Moorpark Office
2400 Moorpark Ave. Suite #300
San Jose, CA 95128

> and primary insureds; (2) The incident did not affect any payment card, bank account, or other financial information.

As of December 11, 2025, OCHIN still did not confirm whether or not any patients of AACI were impacted.

On December 12, 2025, OCHIN informed AACI that you and other patients of AACI were impacted by the data breach.

What Information Was Involved?

According to TPS, the affected data may have included your name, address, date of birth, Social Security number, health insurance member number (which, for some individuals, may be a Medicare beneficiary identifier), provider name, health insurer name, primary insured information, and other demographic, health, and health insurance information. TPS reports that the incident did not affect any payment card, bank account, or other financial information.

What We Are Doing.

TPS reports that it took the following measures during October and November 2025:

> After becoming aware of the incident, TPS immediately took additional protective measures to safeguard its systems and worked with leading cybersecurity experts to conduct a comprehensive investigation of the incident. TPS notified law enforcement and is cooperating with their investigation. TPS has eliminated the threat to the environment. To help prevent similar incidents from happening in the future, TPS implemented and is continuing to implement additional security protocols designed to enhance the security of its services.

AACI wants you to be confident in your data, so we have demanded that TPS do more for AACI patients who were affected TPS's breach. TPS has agreed to provide Single Bureau Credit Monitoring, Single Bureau Credit Report, Single Bureau Credit Score, and proactive fraud assistance services at no charge for a period of 12 months. TPS will provide these services through Kroll, a company specializing in fraud assistance and remediation services. For more information about Kroll, you can visit info.krollmonitoring.com. TPS has agreed that it will mail you a letter on February 9, 2026, that will provide you instructions for enrolling in Kroll's services.

What You Can Do.

During the days after February 9, 2026, be on the lookout for the letter from TPS. Take care to open all mail that you receive during that time, even if it appears to be junk mail. Keep a copy of the letter in a safe place. The letter will contain a unique code that you can use to enroll in Kroll's services.

There will be a limited time to enroll in Kroll's services, so please enroll promptly after you receive the letter from TPS. The enrollment will require an internet connection and email account and may not be

Moorpark Office
2400 Moorpark Ave. Suite #300
San Jose, CA 95128

available to minors under the age of 18. When signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

If you do not receive a letter from TPS by February 16, 2026, please contact TPS's incident support hotline at (844) 572-2724, during Monday through Friday, from 8:00 a.m. to 5:30 p.m., Central Time, excluding major U.S. holidays.

Because your Social Security number may have been involved, in order to protect yourself from the possibility of identity theft, we recommend that you also place a fraud alert on your credit files and order copies of your credit reports by following the recommended privacy protection steps outlined in the enclosed guide titled "Breach Help: Consumer Tips from the California Attorney General." Check your credit reports for any accounts that you do not recognize. If you find anything suspicious, follow the instructions found in section number four of the guide.

Since your health insurance information was also involved, we also recommend that you regularly review the explanation of benefits (EOB) statements that you receive from your health insurance provider. If you see any service that you believe you did not receive, call the contact number listed on the EOB statement. If you do not receive regular EOB statements, contact your health insurance provider and ask them to send EOB statements when they provide services in your name or under your plan number.

More Information.

If you have questions, you may call AACI at (408) 975-2730 ext. 3344. However, we have limited information, because the breach originated from TPS's web portal. This letter already contains substantially all of the information that TPS has provided to AACI regarding the incident, so far.

If you need additional information beyond that contained in this letter, please consider contacting TPS's incident support hotline at (844) 572-2724, during Monday through Friday, from 8:00 a.m. to 5:30 p.m., Central Time, excluding major U.S. holidays.

The letter TPS will send you on February 9, 2026, will also contain a toll-free number specifically for providing information to individuals affected by the incident. When you call that number, be prepared to provide the unique code contained in the letter.

We understand that this is an inconvenience to you. We sincerely apologize and regret that this situation has occurred. AACI is committed to providing quality care, including protecting your personal information, and we want to assure you that we have policies and procedures to protect your privacy.

Sincerely,

AACI Executive Leadership Team

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.