February 9, 2015

To: All KCOE Employees

From: Stephen Corl, Assistant Superintendent

Re: Anthem Security Breach

As you may have heard on news reports and e-mails, Anthem has reported a security breach of personal information that may affect you and all of your covered dependents. This is follow-up to our e-mail sent out to all KCOE employees on Friday, February 6, 2015 and Monday, February 9, 2015.

Initial investigation by Anthem indicates that the member data accessed included names, dates of birth, member ID/social security numbers, addresses, phone numbers, email addresses and employment information. KCOE does not know the details of the date of the breach or how it occurred. Anthem is working to identify the members impacted and will begin to mail letters to impacted members in the coming weeks.

When an employee enrolls for health insurance, they complete the SISC form that can also include spouse and dependents. KCOE sends that form onto SISC, which then SISC enters onto the Anthem Blue Cross system. The security breach is from Anthem. The breach could include your personal information and that of your covered dependents. KCOE does not maintain information about covered dependents so please share this notice with your covered dependents.

In regards to the Cyber-Attack against Anthem Blue Cross, we still do not have any additional information to provide but you can call the toll-free number, 1-877-263-7995 or refer to the FAQ provided at http://www.anthemfacts.com (which is also included). As we hear more, we will pass it on.

Anthem will contact members via mail delivered by the U.S.Postal Service about the cyber-attack with specific information on how to enroll in credit monitoring and those affected will receive free credit monitoring and ID protection services.

Also attached are consumer tips on responding to a security breach. It has practical steps that a consumer can follow to respond to a data breach, including the toll-free numbers of the major credit reporting agencies.

In the meantime, you should be prepared for the scam of email campaigns that may occur. These scams are designed to capture personal information ("phishing") and may appear to be from Anthem. Included is a page of how to be vigilant about scams and phishing.

If you have any questions for me, phone me at 584-1441, ext. 7091 or email at scorl@kings.k12.ca.us.

Attachments

- Scams and Phishing
- Anthem Facts
- Attorney General's Breach Help: Tips for Consumers

Posted on KCOE intranet 2/9/2015
E-mailed to all KCOE employees on 2/9/2015

Scams and Phishing

You should be prepared for the scam of email campaigns that may occur. These scams are designed to capture personal information ("phishing") and may appear to be from Anthem. The emails may include a "click here" link for credit monitoring, see email sample below. These emails are NOT from Anthem. Do NOT click on any links in the email.

Some points to consider:

- Do NOT reply to the email or reach out to the senders in any way.
- Do NOT supply any information on the website that you may open (if you have clicked on a link in an email)
- Do NOT open any attachments that arrive with the email
- Do NOT furnish any personal information to someone if you are contacted by phone
- DO Monitor your existing accounts for unauthorized activity
- DO Stay vigilant – You never know when stolen identity information will be used so you must stay alert

Whether your information was breached or not, you may still be a target for this. Anthem will NOT call members regarding the cyber-attack and is NOT asking for credit card information or social security numbers over the phone. This outreach is from scam artists who are trying to trick consumers into sharing personal data. There is no indication that the scam email campaign is being conducted by those that committed the cyber-attack or that the information accessed in the attack is being used by scammers.

Anthem will contact members via mail delivered by the U.S.Postal Service about the cyber-attack with specific information on how to enroll in credit monitoring and those affected will receive free credit monitoring and ID protection services.

If in doubt regarding a phone call or email, call the Anthem number at 1-877-263-7995.

Was my information accessed?

Anthem is currently conducting an extensive IT Forensic Investigation to determine what members are impacted. We are working around the clock to determine how many people have been impacted and will notify all Anthem members who are impacted through a written communication.

What information has been compromised?

Initial investigation indicates that the member data accessed included names, dates of birth, member ID/ social security numbers, addresses, phone numbers, email addresses and employment information.

Who is responsible for this cyber attack or breach?

Anthem is working closely with federal law enforcement investigators. At this time, no one person or entity has been identified as the attacker.

When will I receive my letter in the mail?

We continue working to identify the members who are impacted. We will begin to mail letters to impacted members in the coming weeks.

How can I sign up for credit monitoring/identity protection services?

All impacted members will receive notice via mail which will advise them of the protections being offered to them as well as any next steps.

Do the people who accessed my information know about my medical history?

No - our investigation to date indicates there was no diagnosis or treatment data exposed.

Do the people who accessed my information have my credit card numbers?

No, our current investigation shows the information accessed did not include credit card numbers.

Did this impact all lines of Anthem Business?

Yes, all product lines are impacted.

Is my (plan/brand) impacted?

The impacted (plan/brand) include Anthem Blue Cross, Anthem Blue Cross and Blue Shield, Blue Cross and Blue Shield of Georgia, Empire Blue Cross and Blue Shield, Amerigroup, Caremore, Unicare, Healthlink, and DeCare.

How can I be sure my personal and health information is safe with Anthem, Inc.?

Anthem is doing everything it can to ensure there is no further vulnerability to its database warehouses. Anthem has contracted with a global company specializing in the investigation and resolution of cyber attacks. We will work with this company to reduce the risk of any further vulnerabilities and work to strengthen security.

The Attorney General's Breach Help: Tips for Consumers has simple instructions for consumers who have been affected by a breach and includes what to do in response to a Social Security number breach. Breach Help is also available in Spanish.

Steps for Responding to Social Security Number Breach:

1. PLACE A FRAUD ALERT.

Contact the three major credit bureaus and place a 90 day "fraud alert." This 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 an "alert" that there may be fraud on the account.

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

You will reach an automated telephone system. You will also be sent instructions on how to get a free copy of your report from each of the credit bureaus. Order the reports.

2. REVIEW YOUR CREDIT REPORTS.

Look through each one carefully. Look for accounts you do not recognize, especially accounts opened since December 2014, when the Anthem breach occurred. Follow the instructions in the report for disputing any questionable information.

3. CONSIDER A SECURITY FREEZE.

Placing a security freeze on your credit files offers longer term protection. For information on how to do this, see "How to Freeze Your Credit Files" at www.oag.ca.gov/privacy/info-sheets.

4. BE WARY OF PHISHING ATTEMPTS.

If you get an email or call from someone claiming to be from Anthem and asking for your personal information, do not provide it. Scammers often take advantage of breaches by offering to help and actually seeking to steal your information. Check with Anthem through the phone number you usually use or one from the phone book, if you want to confirm that such a contact is legitimate.

More consumer information from the Attorney General:

Breach Help: Tips for Consumers
www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/cis-17-breach-help.pdf?
En Español: Ayuda en caso de robo de datos confidenciales
www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/sp-cis-17-breach-help.pdf?
How to Order Your Free Credit Reports
www.oag.ca.gov/sites/all/files/agweb/pdfs/idtheft/cis_11_free_annual_doj...
En Español: Cómo encargar sus informes de crédito gratuitos
www.oag.ca.gov/sites/all/files/agweb/pdfs/idtheft/cis11spanish.pdf?
How to "Freeze" Your Credit Files
www.oag.ca.gov/sites/all/files/agweb/pdfs/idtheft/cis_10_credit_freeze_d...?
Identity Theft Victim Checklist
http://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/CIS_3_victim_checkl...?
En Español: Lo que deben hacer las víctimas de robo de identidad
www.oag.ca.gov/sites/all/files/agweb/pdfs/idtheft/sp_cis_3_vtm_checklist...?
Top 10 Tips for Identity Theft Protection
www.oag.ca.gov/sites/all/files/agweb/pdfs/idtheft/cis_1_top_10tips_doj.pdf?
En Español: Los 10 consejos para protegerse contra el robo de identidad
www.oag.ca.gov/sites/all/files/agweb/pdfs/idtheft/cis_1_top_10tips_doj_s...?