American Apparel®

Crafted With Pride
in the USA

American Apparel, Inc.
HQ/Factory
747 Warehouse St.
Los Angeles, CA 90021
Phone (213) 488-0226
Fax (213) 488-0334

www.americanapparel.net

To: All Employees
From: Craig Simmons / Human Resources Corporate
Re: Information about Anthem's Cyber-Attack
Date: February 19, 2015

As you may have seen in the press, Anthem, Inc. (Anthem), the largest of the Blue Cross and Blue Shield Plans, recently announced it was the target of a sophisticated cyber-attack. In its public announcement, Anthem represents that it immediately began a forensic investigation to determine what personal information may have been impacted and to identify any affected members. Though that investigation is still underway, Anthem states that initial results indicate that certain member data was accessed and that data could include that of American Apparel employees. Anthem has stated that the accessed member data included names, dates of birth, member ID/social security numbers, addresses, phone numbers, email addresses and employment information.

We do know that initial findings in these situations often change and it can take time for Anthem to sort out the details, such as whether in fact our employee data is impacted and, if so, the identity of those employees. There is still much that we do not yet know. Anthem represents that it is still working to determine which members were impacted and will communicate with them directly once those individuals have been identified. We are staying close to the situation and will keep you informed of further developments.

For further information, Anthem has created a dedicated website – www.AnthemFacts.com (http://www.AnthemFacts.com) – where you can access Anthem's information about this event including FAQs. It also provides a dedicated toll-free number, 1-877-263-7995 to address questions about this incident.

In the meantime, please be aware of scams involving emails or telephone calls purporting to be from Anthem. You should be on high alert. Anthem is not communicating with affected individuals by email or by phone and is not asking for credit card or social security numbers.

Anthem will communicate with affected individuals only by regular postal U.S. mail.

Here are some critical scam/hoax email tips to bear in mind:

- DO NOT click on any links in an email that look like they are coming from Anthem.
- DO NOT reply to any Anthem email or reach out to the senders in any way.
- DO NOT supply any information on the website that may open if you have clicked on link in an Anthem-related email.
- DO NOT open any attachments that arrive with Anthem email.
- DO NOT provide any of your personal information over the phone if you receive a call from someone from Anthem.
- DO check your credit card and bank statements for any suspicious charges or entries.
- DO check your credit reports periodically.

Anthem represents that it is providing all members with Identity Theft Protection and Credit Protection for two years at no cost whether or not such members were impacted by the cyber-attack. See www.AnthemFacts.com (http://www.AnthemFacts.com) for details provided by Anthem on how to access and sign up for these services.

Anthem wants to keep you informed about their actions in response to the cyber-attack. If you have given Anthem your email address, you will soon receive an email about identity protection and credit monitoring services. Anthem is required to send this email due to state laws around breach notifications. The subject line of the email will be "Important Message From Anthem, Inc." and it will direct you to visit AnthemFacts.com to sign up for credit protection services. The email will not ask for personal information.
We encourage you to read the email and visit AnthemFacts.com to sign up for the services provided by Anthem.

The following connects to an IRS article that reviews the government's advice on how to avoid tax refund fraud: http://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft. The IRS suggests you file IRS Form 14039 available at this link http://www.irs.gov/pub/irs-pdf/f14039.pdf alerting the federal government that your social security number has been (or is believed to have been) compromised, to help prevent the IRS from erroneously giving someone else a refund of your tax payments. The following link connects to the California form: https://www.ftb.ca.gov/forms/misc/3552.pdf.

Please feel free to contact the Employee Benefits Department at 213-488-0226 ex 1349 if you have any questions.