Oh Say, Can We Breathe? Anthem Members Await Word on Hacking

By DAN ROSENBLUM | Posted: Monday, February 23, 2015 4:45 pm

Harry Nespoli

Hundreds of thousands of city employees may be eligible for identity-theft-repair and credit-monitoring services after hackers accessed the data of as many as 80 million health-insurance members nationwide. Employees covered by Empire BlueCross BlueShield could be affected by the cyberattack on its parent company, Anthem, one of the largest health-insurance carriers in the country.

Municipal Labor Committee Chair Harry Nespoli said that Anthem is the "primary" health-care provider for city workers and that the company told him it would provide a closer estimate this week of the number of city workers affected.

'Keep Members Informed'

"We're staying on top of it, too, and we're keeping all the unions informed and all the unions are keeping their members informed," he said.

Counting retirees, those ranks may include as many as 350,000 people, according to Mr. Nespoli, though a City Hall official pegged the number closer to 250,000 full-time and part-time workers.

Anthem said the "sophisticated attack" occurred over several weeks last December and the company discovered the unauthorized access on Jan. 29. It publicized the breach about a week later, saying the information includes those covered by an Anthem- or BlueCross BlueShield-affiliated plan dating as far back as 2004.

"These attackers gained unauthorized access to Anthem's IT system and have obtained personal information from our current and former members such as their names, birthdays, medical IDs/Social Security numbers, street addresses, e-mail addresses and employment information, including income data," company President and CEO Joseph Swedish said in a statement. "Based on what we know now, there is no evidence that credit-card or medical information such as claims, test results or diagnostic codes were targeted or compromised."

The FBI is investigating the attack.

Since the breach, the United Federation of Teachers, District Council 37, the Patrolmen's Benevolent Association and several other unions have alerted their members about how to avoid

being targeted by scammers. The city's Office of Labor Relations and the state Department of Civil Service have also warned employees about the hack.

DC 37 'Very Concerned'

DC 37 Executive Director Henry Garrido said in a statement that tens of thousands of the union's members may be affected and that it took "diligent steps to reach out and inform" them via its website, its in-house newspaper, the Public Employee Press, and social-media channels. "We are very concerned about our members' privacy, therefore we have made conserving the integrity of our members' information our most important priority," he said.

Anthem has pledged to notify members by U.S. mail if their information was accessed, and urged members to disregard phone calls and avoid clicking e-mailed links, opening attachments or providing information to people purporting to be from the carrier. Members should not give out credit-card or Social Security information electronically.

Other Insurers Affected?

Those insured under Amerigroup, Caremore, Unicare and BlueCross and BlueShield operations in 14 states may also be affected, the company said.

Anthem is offering two years of free credit monitoring and a service to help identity-theft victims repair any financial losses or damage to their credit scores. Information about those services and updates on the breach are available on the website www.AnthemFacts.com, and a telephone help line at 877-263-7995.