

September 30, 2020

ATTORNEY GENERAL RAOUL ANNOUNCES \$39.5 MILLION SETTLEMENT WITH ANTHEM OVER 2014 DATA BREACH

Settlement Includes More Than \$1.7 Million for Illinois and Requires Anthem to Improve Security Measures

Chicago — Attorney General Kwame Raoul today joined a coalition of 43 attorneys general in announcing a [\\$39.5 million settlement](#) with the health insurance company Anthem Inc. stemming from the massive 2014 data breach that involved the personal information of more than 78 million Americans. Raoul's office was part of the executive committee negotiating the settlement, Illinois and will receive more than \$1.7 million. In addition to the payment, Anthem Inc. (Anthem) has also agreed to a series of data security and good governance provisions designed to strengthen its security practices moving forward.

In February 2015, Anthem disclosed that, beginning in February 2014, cyber attackers had infiltrated its systems using malware installed through a phishing email. The attackers were ultimately able to gain access to Anthem's data warehouse, where they harvested names, dates of birth, Social Security numbers, health care identification numbers, home addresses, email addresses, phone numbers, and employment information for 78.8 million Americans, including more than 1.7 million Illinois residents.

"The Anthem data breach compromised the personal information of more than 1 million Illinois residents," Raoul said. "Today's settlement ensures that Anthem prioritizes protecting consumer data with protections designed to prevent future data breaches. This settlement sends the message that companies will be held accountable for not doing enough to keep consumers' personal information secured."

Under the settlement, Anthem has also agreed to a series of provisions designed to strengthen its security practices, including:

- Prohibiting misrepresentations regarding the extent to which Anthem protects the privacy and security of personal information.
- Implementing a comprehensive information security program, incorporating principles of zero trust architecture, and including regular security reporting to the board of directors and prompt notice of significant security events to the CEO.
- Implementing specific security requirements with respect to segmentation, logging and monitoring, anti-virus maintenance, access controls and two factor authentication, encryption, risk assessments, penetration testing, and employee training, among other requirements.
- Implementing third-party security assessments and audits for three years, as well as requiring that Anthem make its risk assessments available to a third-party assessor during that term.

The scam started by "phishing" for a consumer's personal and financial information by sending phony but official-looking emails that included links designed for the consumer to click on, which triggered malware to be installed on a consumer's computer to steal their information. Phishing scams also originated over the phone when a caller claiming to represent Anthem sought to extract personal or financial information from a consumer.

Privacy Unit Chief Matt Van Hise, Consumer Fraud Bureau Chief Beth Blackston, and Assistant Attorneys General Ronak Shah and Carolyn Friedman handled the settlement for Raoul's Consumer Fraud Bureau.

Joining Raoul in the settlement are the attorneys general of Alaska, Arizona, Arkansas, Colorado, Connecticut, the District of Columbia, Delaware, Florida, Georgia, Hawaii, Idaho, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Michigan, Minnesota, Mississippi, Missouri, Nebraska, New Hampshire, New Jersey, New York, Nevada, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, Tennessee, Texas, Virginia, Washington, West Virginia and Wisconsin.