Westlaw Journal
INSURANCE COVERAGE
Litigation News and Analysis • Legislation • Regulation • Expert Commentary
VOLUME 22, ISSUE 4 / NOVEMBER 4, 2011

*Expert Analysis*

# Indiana Attorney General Settles Data-Breach Case for $100,000

***By Marc J. Lederer, Esq.***
***Willkie Farr & Gallagher***

Indiana Attorney General Greg Zoeller announced a settlement with health insurer WellPoint Inc. July 5 over claims falling under the Indiana Disclosure of Security Breach Act, that arose because of an incident causing WellPoint customers' personal information to became publicly accessible through the company's website. The settlement calls for a $100,000 payment, as well as potential reimbursement to affected customers.[1]

## DATA BREACH

Between Oct. 23, 2009, and March 8, 2010, companies affiliated with WellPoint left WellPoint insurance application submissions publicly visible on an application tracker website. These applications contained customers' Social Security numbers, financial information and health records. A consumer notified WellPoint Feb. 22 that year and again March 8 that records containing personal information were accessible. Upon receiving the notification in March, WellPoint immediately corrected the problem with a security update. The company began notifying 645,000 affected customers nationwide June 18, including 32,051 Indiana residents, about the security breach. Zoeller submitted an inquiry to WellPoint after learning of the breach through news reports, and the company's response was received July 30, 2010.

## SECURITY BREACH ACT CLAIMS

Zoeller sued WellPoint Oct. 29, 2010, claiming the company did not comply with the Security Breach Act, Ind. Code § 24-4.9-3, because the breach notification sent to customers and the attorney general's office was not timely.[2] The Security Breach Act requires companies to provide written notification of data breaches to affected state residents and to the attorney general "without unreasonable delay."

## SETTLEMENT

The settlement requires WellPoint to do the following:

- Make a $100,000 payment to the attorney general's office.[3]
- Agree to comply with the Security Breach Act.

- Admit that WellPoint had a security breach and failed to properly notify the attorney general's office as required by law.
- Provide up to two years of credit monitoring and identity-theft-protection services to Indiana consumers affected by the breach.
- Provide reimbursement to any WellPoint consumer up to $50,000 for any proven losses that result from identity theft stemming from the breach.

According to the settlement agreement, WellPoint has developed new procedures to comply with the Security Breach Act. The company issued a statement July 5, saying it implemented security changes to prevent further breaches and there is no indication that any information that may have been accessed has been used inappropriately.[4]

As a warning to other companies, Zoeller said:

> This case should be a teaching moment for all companies that handle consumers' personal data: If you suffer a data breach, and private information is inadvertently posted online, then you must notify the attorney general's office and consumers promptly. Early warning helps minimize the risk that consumers will fall victim to identity theft.[5]

Zoeller also issued warning letters to 47 companies that delayed issuing notice of security breaches. Businesses with Indiana customers are advised to promptly notify consumers and the attorney general of any unauthorized access to personal data so they do not have to learn about it from a second-hand source.

## RELATED CALIFORNIA ACTION

WellPoint and some of affiliates and service providers reached a preliminary settlement July 12 with the plaintiffs in a California class-action suit stemming from the events of this data breach.[6] As part of the class-action preliminary settlement, the company agreed to offer credit monitoring for two years to all affected individuals, reimburse identity-theft losses up to $50,000 per incident and allow identity-theft claims to be filed until May 31, 2016.

In addition, those making identity-theft claims are eligible for five years of credit monitoring. WellPoint also agreed to donate a total of $250,000 to two nonprofit organizations with the purpose of protecting consumers' privacy online. A settlement fairness hearing is scheduled for Nov. 14 in California's Orange County Superior Court to decide whether to approve the settlement.

## NOTES

1 The settlement agreement is *available at* http://www.in.gov/portal/news_events/files/7_5_11_WellPoint_settlement_MTD_and_Order.pdf

2 This was the first lawsuit filed under the Security Breach Act, which was enacted in 2009.

3 The lawsuit filed by Zoeller originally sought civil penalties of $300,000. The Security Breach Act, however, authorizes a civil penalty of no more than $150,000 per deceptive act.

4 This was not WellPoint's first experience with a breach of consumer personal information. In 2006 the company learned that electronic backup tapes with information on 196,000 consumers had been stolen from a commercial data warehouse service. In March 2007 a WellPoint subcontractor lost a compact disk holding unencrypted personal data on about 75,000 consumers. Additionally, in 2007 a computer disk containing the names, birth dates

and Social Security numbers of 2.9 million Medicaid and children's health care recipients were misplaced during shipment by a data processor.

[5] http://www.in.gov/portal/news_events/71252.htm.

[6] https://www.anthembluecrosssecurity settlement.com/SettlementAgreement.pdf; https://www.anthembluecrosssecuritysettlement.com/PreliminaryApprovalOrder.pdf.

**Marc J. Lederer** is a staff attorney at **Willkie Farr & Gallagher** in New York.