'Egregious' Breach Results in Hefty Settlement

St. Joseph Health System Faces Millions in Costs After Data Exposed on the Web

Although most breach-related class action lawsuits fail, the recent $28 million settlement of a suit stemming from a data breach at St. Joseph Health System in California illustrates that egregious breaches can have serious financial consequences.

See Also: Rethinking Endpoint Security

Legal experts say the case also clearly illustrates the importance of all organizations carefully scrutinizing the adequacy of their information security controls - before it's too late.

In what appears to be one of the most generous settlements to date in a data breach class action lawsuit, nearly 32,000 patients of the California multihospital integrated delivery system whose data was exposed are slated next month to receive at least one check each for about $242, with additional potential cash payouts, for a total of $7.5 million. Plus they can apply for reimbursements of up to $25,000 for out-of-pocket expenses and identity theft related losses incurred as a result of a 2012 data breach, for a total of up to another $3 million.

The payments to breach victims are part of a $28 million settlement of a consolidated class action lawsuit against St. Joseph Health System that was finalized recently by the California Superior Court in Orange County. Other expenses include $4.5 million for ID theft protection for victims and $13 million worth of security investments.

Breach Details

The suit centered around a breach involving medical information of patients at nearly a dozen St. Joseph hospitals that was publicly accessible online using search engines such as Google for about a year starting in February 2011. Without explaining in detail what caused the exposure, the settlement documents note that St. Joseph shut down a SharePoint site that inadvertently made the patients' information accessible on the Web.

Information that was accessible online included, for example, patients' diagnoses lists, active medication lists, lab results and demographic information, according to the settlement documents. Exposed information did not include Social Security numbers, addresses or financial data.

"This is definitely one of the highest [settlements awards] we've seen," says attorney Steven Teppler of the law firm Abbott Law Group, which was not involved with the St. Joseph case, but represented plaintiffs in a class action lawsuit against health plan AvMed tied to a data breach in 2009 that affected 1.2 million individuals.

The AvMed lawsuit ended with a $3 million settlement in 2013 that included award payments of up to $30 each to 460,000 individuals. That settlement amounted to a refund to certain individuals for what AvMed should have spent from their membership premiums on protecting data.

"Unjust enrichment was the issue in the AvMed case," Teppler says. But in the St. Joseph case, "my guess is that the award was so high because the breach was so egregious," Teppler says. "As time goes on,

computation of awards will evolve. Is this high award an outlier, or a precursor to [other high settlement amounts in the future]? We will see."

The St. Joseph case involved complex issues, Teppler says. "How do you compute damages for someone's medical history being available on the Web?" he asks. The St. Joseph patient information was available "for anyone to see ... including people such as prospective employers," he adds.

Why Settle?

Attorney Daniel Robinson of the Newport Beach, Calif.-based law firm Robinson Calcagnie Robinson Shapiro Davis, which represented plaintiffs in the case against St. Joseph, says the award to his clients is "the highest that I know of" for a breach-related lawsuit. "The breach was pretty egregious. The trend in settlements [for breach cases] is meaningful settlements. A lot of corporations want to put these instances behind them."

In a statement provided to Information Security Media Group, St. Joseph Health System says it's "pleased that we could come to a settlement on this issue and regrets any undue concern to our patients. Additionally, since the situation was discovered, we have invested in a number of initiatives to ensure the continued security of patient data, including enhanced data security infrastructure. These measures and more are intended to provide for the safety and security of our patients' information."

Settlement Trends

Security attorney Ron Raether of the law firm Troutman Sanders LLP hopes other organizations pay attention to the potential costs of a breach, as illustrated by the St. Joseph Health settlement.

"Companies need to be better prepared to defend the reasonableness of their procedures, which means vetting carefully what infosec controls are in place and implemented," he says.

"Cases are getting past the early challenges on whether the affected individuals have real-world injuries to proceed to the discovery phase. This does not mean that the plaintiff wins the case. Companies can still argue that class certification is not appropriate and that their infosec procedures were reasonable, as a breach does not mean the hospital did not take reasonable measures to protect the data."

Raether stresses that breach cases "will be valued differently based not only on the possible harm to the effected individuals, but also on the company's ability and willingness to defend its practices."

Compensation for Victims

Under terms of the lawsuit settlement, affected individuals who cash their settlement checks within 90 days could also potentially receive additional rounds of payments depending on how many checks in the previous rounds go uncashed.

Based on a formula specified in the settlement, once the bulk of the $7.5 million settlement payout money is distributed and checks cashed, remaining uncashed funds will be donated to charity.

The settlement also provides for a total of $3 million in reimbursements to victims for losses and out-of-pocket expenses incurred as a result of the breach. "Defendants shall reimburse each participating settlement class member up to $25,000 for any loss that is claimed and shown to have occurred more likely than not as a result of the alleged breach," the settlement states.

Those affected by the breach who are seeking such reimbursement must demonstrate an "actual, documented and unreimbursed loss" that resulted from identity theft due to the alleged breach and that occurred from Feb. 1, 2011, through Jan. 1, 2017.

Those affected by the breach may also seek payments for reimbursement of out-of-pocket expenses, such as the cost of obtaining additional credit monitoring and identity theft insurance beyond the protection previously offered by St. Joseph; the cost of telephone calls and postage related to inquiries on a victim's bank accounts, financial accounts, mortgage accounts and/or credit reports; lost time - calculated at $10 per hour; the cost of placing a freeze on a credit report; and the cost of changing a phone number.

Also, as part of the settlement, five plaintiffs representing the class in the lawsuit will receive payments ranging from $7,500 to $15,000, for a total of $50,000. Plaintiffs' counsel were awarded attorneys' fees and costs up to $7.45 million.

The settlement also states that St. Joseph spent about $4.5 million on one year of identity theft and credit monitoring to all those affected by the breach as well as $13 million on costs related to breach notification, instituting policies to comply with state and federal authorities, and instituting numerous security-related remedial measures.

Remedial Efforts

The settlement documents indicate that St. Joseph's remedial efforts and costs in the wake of the breach included $2 million to retain the consulting firm Deloitte to develop an integrated controls framework and assist in the implementation of a governance, risk and compliance tool to assess application and related systems security. St. Joseph also revamped its security training programs and hired a permanent chief security officer.

St. Joseph also shut down the SharePoint site that inadvertently made the patients' information accessible on the Web. The healthcare provider also attempted to remove all of the search engine links to the data on the SharePoint site and stored cached copies of the data. "To that end, personnel collected and submitted to Google hundreds of unique URL Web addresses associated with the data stored on the SharePoint site. Google then deleted both the search engine links and any cached copies of the data," the court documents state.

St. Joseph hired another consultant to confirm that the search engine links to the origin of the data were identified and removed, the settlement notes.