Published on *The National Law Review* https://natlawreview.com

# Shareholder Seeks Second Look At Company Data Security Practices

Article By:

S. James Boumil, III

On November 25, 2020, a shareholder of First American Financial Corporation ("First American") filed suit against the company and its officers and directors over a massive data security breach that exposed hundreds of millions of sensitive customer records. The shareholder derivative action, filed by Norman Hollett in Delaware federal court, alleges breaches of fiduciary duties, unjust enrichment, abuse of control, gross mismanagement, waste of corporate assets, and multiple violations of the Securities Exchange Act of 1934, all relating to the failure to contain and timely disclose the breach. First American provides real estate financial services such as residential and commercial title insurance. In connection with its business, First American compiles a variety of personally identifiable information, including names, email addresses, mailing addresses, dates of birth, social security numbers, bank account numbers, and other highly sensitive personal information. According to the complaint, to automate the delivery of its products, First American created an application that provided access to an online repository of documents containing this information. Each document was given a sequential ID number that, in turn, was reflected in a URL linking to the document. Under this system, by changing the ID number in the URL for a certain document link by one or more digits, anyone with a web browser could view the document corresponding to the altered ID number.

The complaint alleges the vulnerability persisted for almost five years before it was remedied. More compelling, perhaps, is plaintiff's allegation that the vulnerability was detected during a penetration test conducted in December, 2018, but the company failed to correct the issue or disclose it for almost six months after the test. In fact, the company allegedly was motivated to act only when a prominent cybersecurity blog featured an article in May, 2019 exposing the incident. After publication of the article, the company's stock price fell over 6.2% over the course of one trading day. The complaint also alleges the company's CEO, Dennis Gilmore, sold $5.497 million in company stock after the data security breach but before the scheme was exposed, such that the stock was artificially inflated at the time of sale.

Multiple other actions concerning the same events have also commenced. The SEC opened an investigation on August 7, 2019 to determine whether federal securities laws were violated; the New York State Department of Financial Services filed an enforcement action on July 21, 2020; and a number of consumer class actions were filed on behalf of consumers whose personal information was exposed as a result of the breach. Litigation is just beginning and we will continue to monitor the

case for significant decisions pertaining to data privacy and breach remediation..

The case is Norman Hollett et al. v. Dennis J. Gilmore et al.



National Law Review, Volume X, Number 344