NetDiligence®

State of Litigation

LITIGATION CONFERENCES

Speakers

- Steve Anderson (Moderator), *QBE*
- Matt Meade, *Buchanan Ingersoll & Rooney*
- Dom Paluzzi, *McDonald Hopkins*
- Eve-Lynn Rapp, *Edelson*
- John Yanchunis, *Morgan & Morgan*

Trends & Statistics: Some Empirical Data

The odds of lawsuits occurring following a data breach are:

- 3.5 times greater when individuals suffered financial harm;
- Over 6 times lower when free credit monitoring is offered; and
- 3 times greater for cases involving improperly disposing data than for cases involving stolen data.
- Defendants settle 30% more often when plaintiffs allege financial loss from a data breach, or when faced with a certified class action suit.
- The odds of a settlement are 10 times greater when the breach is caused by a cyber-attack, relative to lost or stolen hardware.
- The compromise of medical data increases the probability of settlement by 31%.

Source: Romanosky, S., *et al.* "Empirical Analysis of Data Breach Litigation", *Journal of Empirical Legal Studies*, Vol. 11, Issue 1, pp. 74-104, March 2014

Important cases

Resnick v. AvMed, Inc.
11th Cir. 2012

Anderson v. Hannaford Bros.
1st Cir. 2011

Neiman Marcus
7th Cir. 2015

Galaria v. Nationwide Mutual Insurance Company
6th Cir. 2016

P.F. Changs
7th Cir. 2016

Target
D. Minn. 2015

Anthem
N.D. Cal. 2016

DAMAGES

- Loss time (Niemen Marcus, PF Changs, *Kuhn v. Capital One Fin.* (Mass. App. Ct. 111, 2006 WL 3007931 at *3))
- Loss of funds through fraudulent charges (Target and Home Depot)
- Loss of interest from false tax returns
- Expense of accountant or tax preparer to assist a taxpayer in addressing a false tax return
- NSF charges
- Benefit of the bargain loss, loss of value of personal information and consequential out of pocket losses (Anthem)
- Damages which consumers would not have incurred had they known of lax security (Target, Anthem, Advanced Data Processing)
- Injunctive Relief: *In Re: Premera Blue Cross Customer Data Security Breach Litigation,* Case No. 3:15-md-2633-SI (D. Oregon, August 1, 2016)

Neiman Marcus – Credit Monitoring

It is telling in this connection that Neiman Marcus offered one year of credit monitoring and identity-theft protection to all customers for whom it had contact information and who had shopped at their stores between January 2013 and January 2014. It is unlikely that it did so because the risk is so ephemeral that it can safely be disregarded. These credit-monitoring services come at a price that is more than *de minimis*. For instance, Experian offers credit monitoring for $4.95 a month for the first month and then $19.95 per month thereafter.See http://www.experian.com/consumer-products/credit-monitoring.html.

That easily qualifies as a concrete injury.

Neiman Marcus – Credit Monitoring

- Organizations should carefully evaluate the decision to offer credit monitoring to impacted individuals in connection with a data breach.
- Credit monitoring in a credit card breach is a sign that the risk was real, not “ephemeral” and, therefore, qualified as a concrete injury.

Shareholder Derivative Claims – Target

- Devise and maintain a system of internal controls sufficient to ensure that customers' personal and financial information was protected.
- Ensure the timely and accurate notification of customers regarding any data breach.
- Remain informed as to how Target conducted its operations.
- Make reasonable inquiry in connection with notice of unsound conditions and take steps to correct.

Shareholder Derivative Claims – Target

- BOD appointed Special Litigation Committee to investigate claims.
- SLC conducted a two-year investigation to evaluate whether Board's conduct ran afoul of standard of care, reviewing thousands of documents and conducting 68 witness interviews. SLC also met with and received information from counsel for the shareholders and for Target.
- SLC issued 91-page report in March detailing extensive data security processes in place before the breach and the post-breach efforts to improve those processes. SLC concluded that it was not in the interest of Target to pursue claims against the officers and directors.
- Derivative Plaintiffs then stipulated that they did not oppose motion to dismiss.
- 7/7/16: Court dismissed claims.

Shareholder Derivative Claims – Wyndham

- Breach of fiduciary duty for failure to implement appropriate security measures even though defendants knew customers were vulnerable to attack
- Waste of corporate assets by failing to implement adequate internal controls to prevent breaches
- Unjust enrichment for compensation received while breaching fiduciary duties.
- BOD appointed Special Litigation Committee to investigate claims.

Shareholder Derivative Claims – Wyndham

Court rejected bad faith/unreasonable investigation claim:

- BOD discussed cyber-attacks at 14 meetings, and GC gave presentation regarding data breaches or security at each meeting.
- Audit committee discussed cyber at 16 meetings.
- FTC investigation helped to develop BOD's understanding.
- Retained third-party technology firms to investigate each breach and recommend enhancements.

Shareholder Derivative Claims – Home Depot

Allegations that BOD was complacent "leaving in place vulnerabilities that not only allowed hackers to enter the system undetected but permitted them to continue siphoning customer cardholder and personal data for almost five months without detection."

Shareholder Derivative Claims – Home Depot

- If we rewind the tape, our security systems could have been better. Data security just wasn't high enough in our mission statement."
- Data security systems were "desperately out of date."

Quotes from former CEO Frank Blake

Shareholder Derivative Claims – Home Depot

- Obligations to devise, implement, oversee and monitor internal controls; ensure timely notice of a breach; establish corporate governance structures to enable oversight.
- Failures of board to implement reasonable measures such as an adequate firewall, to ensure encryption of cardholder data, to install up to date anti virus and malware protections, to limit access to data, and to monitor caused major loss!

Shareholder Derivative Claims – Home Depot

- Motion to dismiss pending based on the following three theories: failure to meet pre suit demand requirements; failure to plead facts that Board consciously failed to monitor cyber; erroneous belief that Board is liable for independent criminal acts.

State Attorney General Enforcement Actions

Alliance Health & Management

Reducing the Risk

- Vendor management
- Document disposal
- Document retention
- Breach response
- Incident Response Plan (IRP)
- Training