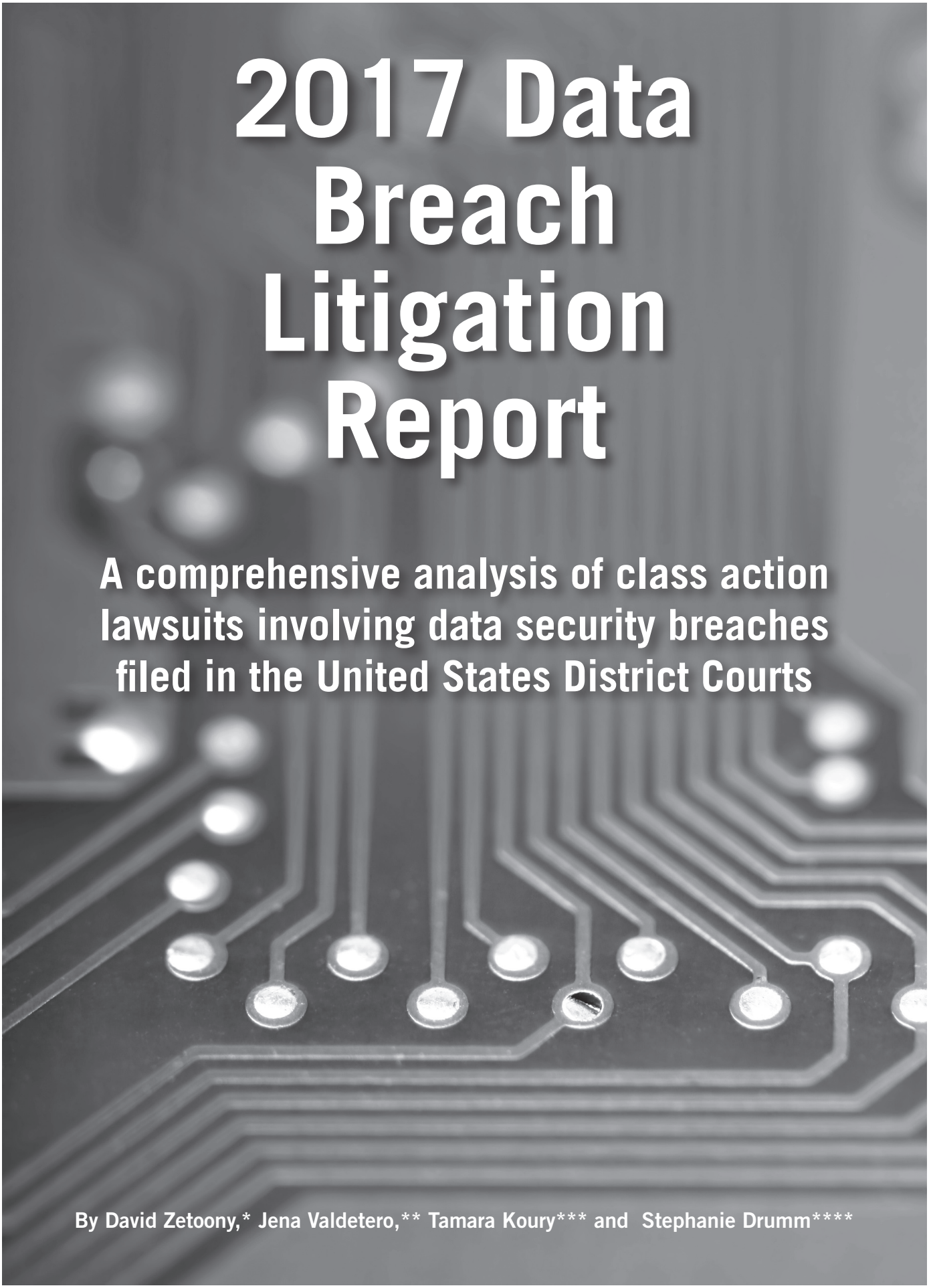


2017 Data Breach Litigation Report

A comprehensive analysis of class action lawsuits involving data security breaches filed in the United States District Courts

By David Zetoony,* Jena Valdetero,** Tamara Koury*** and Stephanie Drumm****

Despite the fact that data breaches do not appear to be going away anytime soon, the risk that a company will face litigation following a data breach remains relatively low year-after-year.

Executive Summary

2016 was another year in which data breaches continued to dominate the headlines, a constant reminder to people that their personal information was vulnerable and the target of criminal attacks. Yet, despite the fact that data breaches do not appear to be going away anytime soon, the risk that a company will face litigation following a data breach remains relatively low year-after-year. The reason is likely tied to the difficulty plaintiffs continue to face establishing that they were injured by a breach and, therefore, have standing as a matter of law to bring suit.

Nonetheless, fear is a powerful marketing strategy, and we continue to see misinformation disseminated to the public about the likelihood of being sued after a data breach. This is not to say that companies should not continue to devote significant resources to breach preparation, information security, and breach response. But we are firm believers in allocating resources in proportion to the risk of harm, and litigation arising from a breach generally does not occur except in cases of public breaches involving large quantities of highly sensitive information.

Bryan Cave LLP began its survey of data breach class action litigation five years ago to rectify the information gap and to provide our clients, as well as the broader legal, forensic, insurance, and security communities, with reliable and accurate information concerning the risk associated with data breach litigation. Our annual survey continues to be the leading authority on data breach class action litigation and is widely cited throughout the data security community.

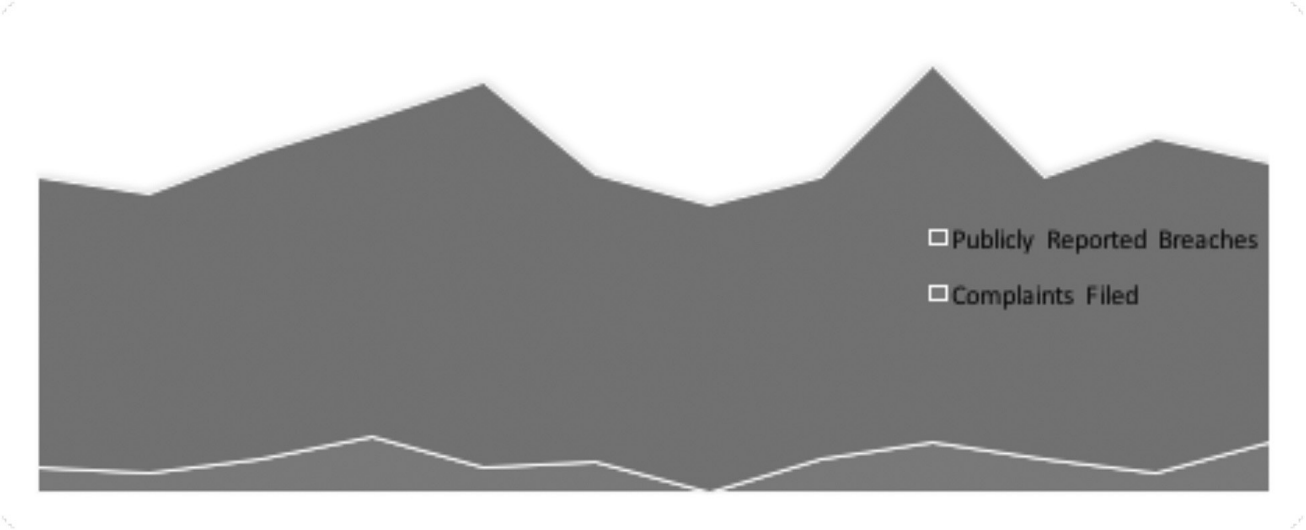
Our 2017 report covers federal class actions initiated over a 12 month period from January 1, 2016 to December 31, 2016 (the "Period"). Our key findings are:

- Modest increase in filings. 76 class actions were filed during the Period. This represents a modest **7% increase in the quantity of cases filed as compared to the 2016 Data Breach Litigation Report** (the "2016 Report").
- Continued "lightning rod" effect. Consistent with prior years, many of these lawsuits cluster around the same high-profile breaches. When multiple filings against single defendants are removed, **there were only 27 unique defendants during the Period**. This indicates a continuation of the "lightning rod" effect noted in previous reports, wherein plaintiffs' attorneys file multiple cases against companies who had the largest and most publicized breaches, and generally bypass the vast majority of other companies that experience data breaches.
- Decrease in filings as a function of the quantity of breaches. Approximately 3.3% of publicly reported data breaches led to class action litigation. Unlike in prior years, in which the percentage of class action lawsuits has remained relatively steady at 4 or 5% of publicly reported breaches, **2016 saw a slight decrease in litigation relative to the number of breaches**.
- Litigation forums cluster around location of defendants. The Northern District of California, the Middle District of Florida, and the District of Arizona were the most popular jurisdictions in which to bring suit in 2016. **Choice of forum, however, continues to be primarily motivated by the states in which the company-victims of data breaches are based**.
- Medical industry disproportionately targeted by the plaintiffs' bar; but may still be underweighted. Like the previous year, **the medical industry was disproportionately targeted by the plaintiffs' bar**. Although 70% of publicly reported breaches related to the medical industry, only 34% of data breach class actions targeted the medical industry or health insurance providers.
- Credit card breach litigation is flat. **The percentage of class actions involving the breach of credit cards stayed relatively constant as compared to the 2016 Report,** with credit and debit cards data accounting for 21% of the type of data involved in data breach class actions in 2016, slightly down from 23% for the previous reporting period. This may reflect the lack of high profile credit card breaches as in past years, difficulties by plaintiffs' attorneys proving economic harm following such breaches, and relatively small awards and settlements in previous credit card related litigation.
- Plaintiffs continue to experiment with legal theories. Plaintiffs' attorneys continue to allege multiple legal theories. **Plaintiffs alleged a total of 21 legal theories during this period**.
- Negligence has emerged as the clear theory of preference. While negligence was the most popular legal theory in the 2016 (and 2015) Report, **it has increased from being included in 75% of cases to being included in nearly 95% of all cases**.
- Plaintiffs are focusing on sensitive categories of information. Plaintiffs' attorneys overwhelmingly focused on breaches in this Period that involved information such as Social Security Numbers, medical treatment information, health insurance information, and security questions and answers, **with 89% of cases in 2016 involving a breach of sensitive data**.

Part 1: Volume of Litigation

A total of 76 complaints were filed during the Period, up 7% from the 2016 Report. The quantity of litigation loosely correlates with the number of publicly reported breaches each month. For example, of the months studied in the Period, September 2016 was the month that saw the highest number of publicly reported data breaches. September (along with April) also saw the greatest percentage of complaints filed.

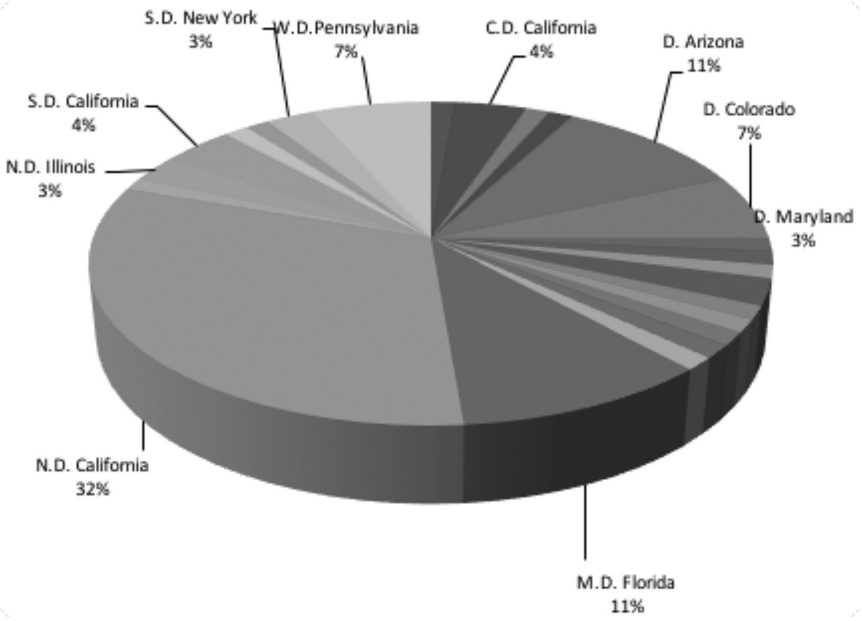
According to the Privacy Rights Clearinghouse Chronology of Data Breaches, 806 breaches were publicly reported during the Period. However, only 76 federal class action complaints were filed during the same timeframe, and these filings related to only 27 unique defendants. As a result, approximately 3.3% of publicly reported breaches led to class action litigation. The overall result is that there has not been an increase in the rate of complaint filings when total complaints are normalized by the quantity of breaches. The following chart provides a breakdown of class action complaints filed with the quantity of publicly reported breaches disclosed during the Period:



Part 2: Favored Courts[6]

The Northern District of California is the preferred forum for filing data breach class action litigation, with almost 40% of all filings originating in that court. However, the high rate was attributable to the fact that 25 of the 76 complaints were filed against Yahoo!, Inc., which is headquartered in Silicon Valley. The concentration of litigation seems to be related to the location of headquarters of the company that encountered the breach. For example, for the first time, we saw an increase in lawsuits filed in Arizona, however, this was due to cases filed against Banner Health, an Arizona company. Similarly, litigation was prevalent in Florida due to a breach involving 21st Century Oncology Holdings, a Florida company.

The following provides a detailed breakdown by district of federal class action filings:[7]

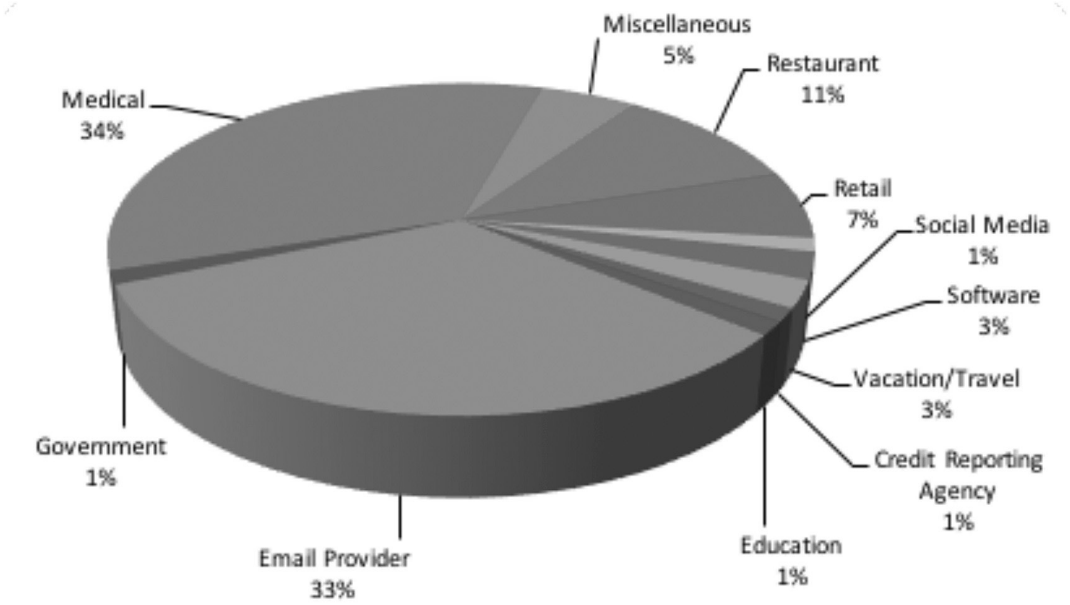


Part 3: Litigation by Industry

The medical industry was the target of the majority of class action complaints (34%), with 26 complaints filed during the Period, a slight decrease from the 2016 Report findings. The retail industry was the target of only 7% of complaints, a slight decrease from the 2016 Report.

2016 saw the emergence of multiple class actions against Yahoo!, Inc. related to disclosure of two major security breaches involving 500 million users and more than 1 billion user accounts. The Restaurant Industry also emerged as a target of class action complaints, with six class actions filed against The Wendy's Company and two against Noodles & Company. In contrast, the consumer reporting agencies saw a steep decline in class actions given the lack of new filings against Experian Information Solutions, which was heavily targeted in 2015.

The following chart provides a detailed breakdown of class action complaint filings by industry sector:

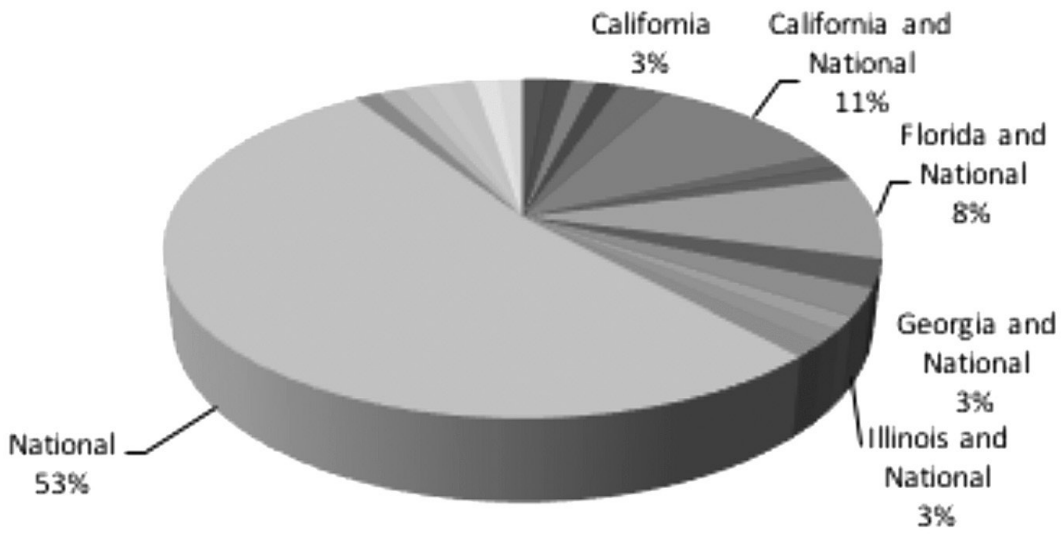


Part 4: Scope of Alleged Class (National v. State)

Access to class action complaints filed in state court differs among states and, sometimes, among courts within the same state. As a result, it remains difficult, if not impossible, to identify the total quantity of class action filings in state court, and any analysis that includes state court filings would include a significant and misleading skew toward states that permit easy access to filed complaints. As a result, we purposefully do not include state court filings in our analysis and instead focus only on complaints filed in federal court and complaints originally filed in state court but subsequently removed to federal court under the Class Action Fairness Act ("CAFA") or federal question jurisdiction.

We find in our dataset a strong preference for class actions that are national in scope. This may mean that plaintiffs' attorneys prefer to allege putative national classes in an attempt to obtain potentially greater recovery. It could also reflect the fact that many companies collect data from individuals without regard to geography. It could also mean, however, that additional complaints that have not been included in our analysis were filed in state court alleging putative classes comprised of single state groups.

Despite the preference for national classes, we again see almost half of complaints allege sub-classes tied to residents in specific states.[8] The following provides a detailed breakdown of the scope of putative classes:[9]

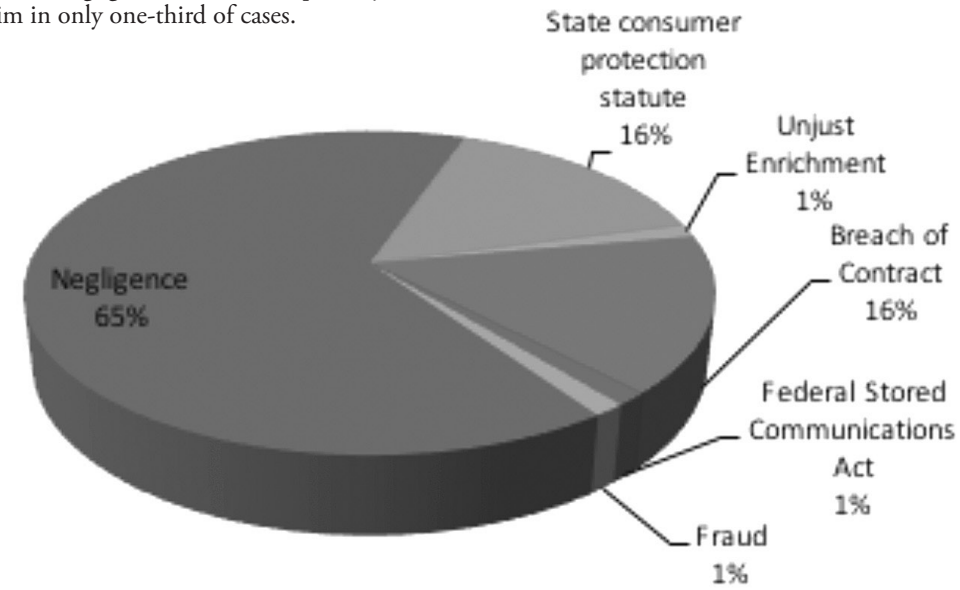


Part 5: Primary Legal Theories

Plaintiffs continue to pursue negligence as the predominate theory under which they sought recovery, with 65% of all class action litigation alleging negligence as the primary theory (*i.e.*, the first count alleged in a complaint), and 95% of all complaints including it as a cause of action. This increase continues a trend from the 2016 Report, in which negligence was also the primary theory, but was the lead claim in only one-third of cases.

Despite 48 states having enacted a data breach notification statute, not a single plaintiff alleged violation thereof as the primary legal theory, although 27% included a violation of the state breach notification statute as a supplemental cause of action.

The following provides a breakdown of the primary theory alleged:



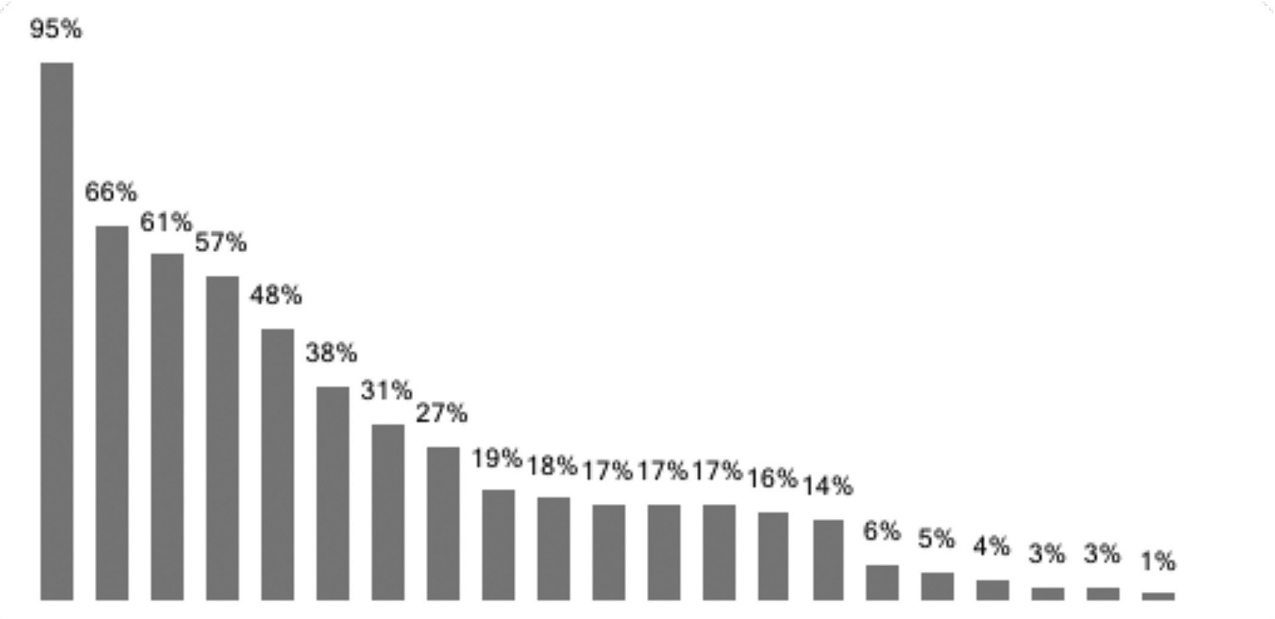
Part 6: Variety of Legal Theories Alleged

Although negligence was the most common theory first put forward by a plaintiff's attorney, most plaintiffs chose to allege more than one theory of recovery, and many plaintiffs' attorneys included theories sounding in contract, tort, and statute.

As indicated in the table below, although plaintiffs' attorneys show a clear preference for some legal theories – *e.g.,* breach of contract, negligence, and state consumer protection statutes – in total they have pursued 21 different legal theories of recovery. "Bailment" or the idea that plaintiffs delivered their private information to defendants and therefore defendants owed them a duty to safeguard the information emerged as a trend in the 2016 Report. That trend continues with bailment alleged in approximately one-fifth of complaints. There has also been an uptick in cases asserting counts for Breach of Covenant of Good Faith and Fair Dealing, which is a derivative breach of contract claim.

The following chart provides a detailed breakdown of the theories utilized by plaintiffs' attorneys in data breach litigation complaints:

Part 7: Primary Type of Data at Issue



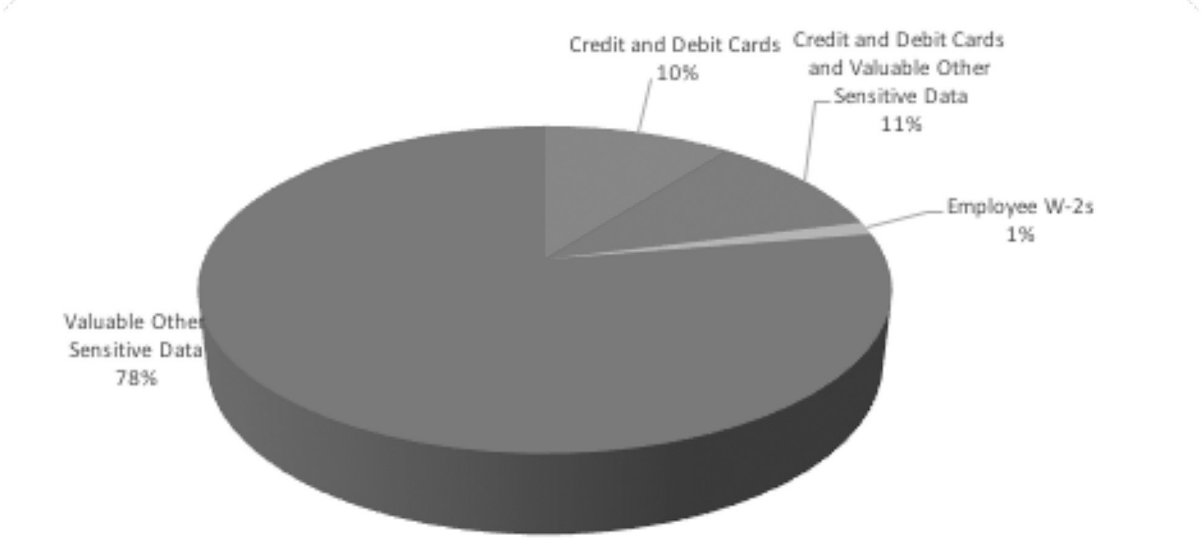
Data drawn from medical records has become the single largest focus of both publicly reported breaches and class action lawsuits. It is no surprise that this industry is increasingly targeted and affected by hacking and data breaches given that it is a $3 trillion industry and accounted for 17.8% of the GDP in 2015.[10]

While 70% of publicly reported breaches involved the medical industry, only 34% of data breach litigation related to this industry. Although the relatively low percentage of lawsuits compared to publicly reported breaches could be considered reassuring, we expect that breaches in the medical industry and class action lawsuits resulting from those breaches will continue to represent a large percentage compared to other industries. Our expectation is based upon a number of factors, including the fact that medical data is reportedly worth substantially more than credit card information on the black market (some estimate 10 times more).[11] This relative value is in part due to the greater amount of personal data contained in health records and because such records have a longer shelf-life compared to credit cards, where the fraud is usually discovered more quickly and the card cancelled.

Despite the value of the data and the fact that it is increasingly targeted, the healthcare industry notoriously spends a low percentage of its budget on security (by some reports, only 1 to 2% on data security) which is significantly less than other sectors, such as the financial sector.[12] Add to that the rapidly increasing role of technology in this industry generally, including increased use of electronic medical records, internet dependent medical devices and the expansion of digital health care, and you have the perfect storm for data breach targets. In addition, there is a focus on health record "interoperability" to promote sharing and access of health information by providers and the patient, as well as value-based reimbursement that promotes collaboration and data sharing between providers. While these are positive developments for health care generally, they present increased data security related risks.

Meanwhile, the trend of decreasing focus on breaches that involved credit cards has continued. The quantity of class actions relating to credit cards declined by 2 percentage points from 23% to 21%. This decrease is likely the result of fewer high profile retail breaches during the Period, as well as difficulties for plaintiffs' attorneys to prove compensable injury in a credit card related data breach. Specifically, the Fair Credit Billing Act ("FCBA") and the Electronic Fund Transfer Act ("EFTA") dictate that a consumer cannot be held responsible for more than $50 in charges so long as the consumer reports the loss or theft of their card (or the unauthorized activity) within two business days of learning about it.[13] In addition, because many banks and payment card networks now voluntarily waive even the $50 most consumers suffer no financial harm as a result of a breach that involves their credit card.

The following chart provides a detailed breakdown of the type of data involved in data breach litigation:



Part 8: Plaintiffs' Firms
More than 72 plaintiffs' firms participated in filing class action complaints related to data security breaches. Although one plaintiffs' firm filed six class action lawsuits, the majority filed only one or two complaints.

Part 9: Methodology
The data analyzed in this report includes consumer class action complaints that were filed against private entities. Complaints that were filed on behalf of individual plaintiffs were excluded.

Data was obtained from the Westlaw Pleadings, Westlaw Dockets, Bloomberg Law, and PACER databases. The sample Period covered January 1, 2016-December 31, 2016. Multiple searches were run in order to find complaints that included – together with "class action" -- the following search terms:

- "security," or "breach" and phrases containing "personal," "consumer," or "customer" at a reasonable distance from the words "data," "information" or it derivations, "record," "report," "email," "number," or "code," or
- "data" at a reasonable distance from "breach,"

Although additional searches were conducted using the names of businesses that were the target of major data breaches (*e.g.*, "Yahoo" and "breach") not all of the complaints filed as a result of these data breaches were found using Westlaw. Any discrepancy may be due in part to the speed at which the multiple filings were consolidated.

All the complaints identified by these searches were read and, after the exclusion of non-relevant cases, categorized in order to identify and analyze the trends presented in this report.

As was the case in Bryan Cave's prior whitepapers, state complaints have been excluded so as not to inadvertently over-represent or under-represent the quantity of filings in any state. Complaints that were removed from state court to federal court were included within the analysis.

** Attorney Bryan Cave. David Zetoony is the leader of Bryan Cave's Data Privacy and Security Team. David's practice focuses on advertising, data privacy, and data security and he co-leads the firm's Data Breach Response Team.*

*** Attorney Bryan Cave. Jena Valdetero is the co-leader of Bryan Cave's Data Breach Response team, which focuses on counseling, compliance, and litigation. In her work in this area, she helps companies take the appropriate actions before, during, and after a data breach.*

**** Attorney Bryan Cave. Tamara Koury has significant experience defending and counseling businesses across many industries and has a particular interest in the healthcare industry and the privacy, security and regulatory compliance issues it faces.*

***** Attorney Bryan Cave. Stephanie Drumm is a member of Bryan Cave's Data Privacy and Security Team and a graduate of the University of Colorado at Boulder school of law.*

---

1 Although the 2016 Report indicated that there were 83 cases filed, that number was for a 15-month period. Normalized for a 12-month period, this would have been 71 cases for 2015 as compared to 76 cases for 2016. *See* Bryan Cave LLP, 2016 Data Breach Litigation Report: A Comprehensive Analysis of Class Action Lawsuits Involving Data Security Breaches Filed in United States District Courts.

2 Privacy Rights Clearinghouse estimates that in the Period, 566 of the 806 publicly reported breaches involved the medical industry. *See* http://www.PrivacyRights.org (last viewed August 9, 2017).

3 The 2016 Data Security Report is available at: http://bryancavedatamatters.com/category/white-papers/white-papers-security/.

4 *See* Privacy Rights Clearinghouse Chronology of Breaches available at http://www.privacyrights.org (last viewed August 9, 2017).

5 *Id.*

6 This report does not include complaints filed in state courts. For more information, please see Part 9: Methodology below.

7 The following courts are not labeled in the chart and each represent 2% of the total filings during the Period: Southern District of Illinois, Southern District of Florida, Kansas District Court, Georgia District Court, Louisiana District Court, Missouri District Court, Tennessee District Court, Central District of Illinois, Eastern District of Louisiana, Massachusetts District Court, Eastern District of Michigan, Northern District of Georgia..

8 The 2016 Data Security Report found that almost half of complaints alleged a subclass.

9 The following scopes of putative classes are not labeled in the chart and each represent less than 2% of the total filings for the Period: Arizona and National; Arkansas; Arkansas and National; Australia; Colorado and National; Colorado, Texas, Maryland, California, New Jersey and National; Illinois, Maryland, New Jersey and National; Kansas and National; Massachusetts, Florida and National; Montana; Mexican Nationals, New Jersey and National, New York; North Carolina and National; Ohio and National; and Utah.

10 Centers for Medicare & Medicaid Services, National Health Expenditure Data, https://www.cms.gov/Research-Statistics-Data-and-Systems/Statistics-Trends-and-Reports/NationalHealthExpendData/NationalHealthAccountsHistorical.html.

11 Caroline Humer, Jim Finkle, *Your medical record is worth more to hackers than your credit card*, Reuters (September 24, 2014), http://www.reuters.com/article/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924.

12 Michael Ash, *The Conundrum of Health Care Security Spending*, SecurityIntelligence (May 2, 2017), https://securityintelligence.com/the-conundrum-of-health-care-security-spending/.

13 *See* FTC Information Sheet, Lost or Stolen Credit, ATM, and Debit Cards *available at* http://www.consumer.ftc.gov (last viewed August 9, 2017).