2016 Data Breach Litigation Report

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

BRYAN CAVE

Executive Summary

Data security breaches – and data security breach litigation – dominated the headlines in 2015 and continue to do so in 2016. Continuous widely publicized breaches have led to 30,000 articles a *month* being published that reference data breach litigation. Law firms have collectively published more than 156,000 articles on the topic.[1]

While data breach litigation is an important topic for the general public, and remains one of the top concerns of general counsel, CEOs, and boards alike, there remains a great deal of misinformation reported by the media, the legal press, and law firms. At best this is due to a lack of knowledge and understanding concerning data breach litigation; at worst some reports border on sensationalism or fearmongering.

Bryan Cave LLP began its survey of data breach class action litigation four 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 data breach litigation risk. We are proud that our annual survey has become the leading authority on data breach class action litigation and is widely cited throughout the data security community.

Our 2016 report covers litigation initiated over a 15 month period from the fourth quarter of 2014 through the fourth quarter of 2015 (the "Period").[2] Our key findings are:

- 83 cases were filed during the Period. This represents a nearly ***25% decline in the quantity of cases filed as compared to the 2015 Data Breach Litigation Report*** (the "2015 Report").[3]

- When multiple filings against single defendants are removed, there were only 21 unique defendants during the Period. This indicates a continuation of the "lightning rod" effect noted in the 2015 Report, wherein plaintiffs' attorneys are filing multiple cases against companies connected to the largest and most publicized breaches, and are not filing cases against the vast majority of other companies that experience data breaches. As with the overall quantity of cases filed, the quantity of unique defendants also declined as compared to the 2015 Report*;* approximately ***16% fewer unique defendants were named in litigation***.

- Approximately 5% of publicly reported data breaches led to class action litigation. The conversion rate has remained relatively consistent as compared to prior years. The stability in the conversion rate is explained by a decrease in the number of publicly reported data breaches. While further research would be needed to separate correlation from causation, it

---

1 Google News Search for "Data Breach Litigation" conducted on March 22, 2016 (covers 30 days); Lexology.com search for "Data Breach Litigation" conducted on March 25, 2016.

2 The study period included October 1, 2014 through December 31, 2015.

3 Complaints filed against Government agencies were excluded from the 2015 report and included in the 2016 report. Therefore, the decline in overall complaints filed would be even further pronounced if Government agencies were excluded from the 2016 Report. *See* Bryan Cave LLP, 2015 Data Breach Litigation Report: A Comprehensive Analysis of Class Action Lawsuits Involving Data Security Breaches Filed in United States District Courts.

appears that ***the decline in the absolute quantity of data breach class action litigation, and the absolute quantity of data breach class action litigation defendants, may be primarily due to a decline in the overall quantity of reported breaches***. At this point there is no evidence to suggest that the decline in litigation is attributable to other causes (*e.g.,* disinterest by the plaintiff's bar, lack of success of previous litigation, etc.).

- The Northern District of Georgia, the Central District of California, the Northern District of California, and the Northern District of Illinois are the most popular jurisdictions in which to bring suit. ***Choice of forum, however, continues to be primarily motivated by the states in which the company-victims of data breaches are based***.

- Unlike in previous years, ***the medical industry was disproportionately targeted by the plaintiffs' bar***. While only 24% of publicly reported breaches related to the medical industry, nearly 33% of data breach class actions targeted medical or insurance providers.[4] The overweighting of the medical industry was due, however, to multiple lawsuits filed in connection with two large scale breaches. As a result, we do not expect the overweighting of the medical professions for breach litigation to necessarily continue into the coming year.

- There was a ***76% decline in the percentage of class actions involving the breach of credit cards*** as compared to the 2015 Report. The decline most likely reflects a reduction in the quantity of high profile credit card breaches, difficulties by plaintiffs' attorneys to prove economic harm following such breaches, and relatively small awards and settlements in previous credit card related breach litigation.

- While plaintiffs' attorneys continue to allege multiple legal theories, there appears to be some movement toward consolidation. For example, although ***plaintiffs alleged 20 legal theories, that represents a 16% decline from the 2015 Report***, which identified 24 legal theories.

- Favored legal theories continue to emerge. Specifically, while negligence was the most popular legal theory in the 2015 Report, with 67% of cases including a count of negligence, ***nearly 75% of cases now include a count of negligence***.

- Unlike in previous years in which plaintiffs' attorneys focused on breaches of information that was arguably of a less sensitive variety (*e.g.,* credit card numbers), ***plaintiffs' attorneys overwhelmingly focused on breaches in this Period that involved information that is traditionally considered "sensitive"*** such as Social Security Numbers.

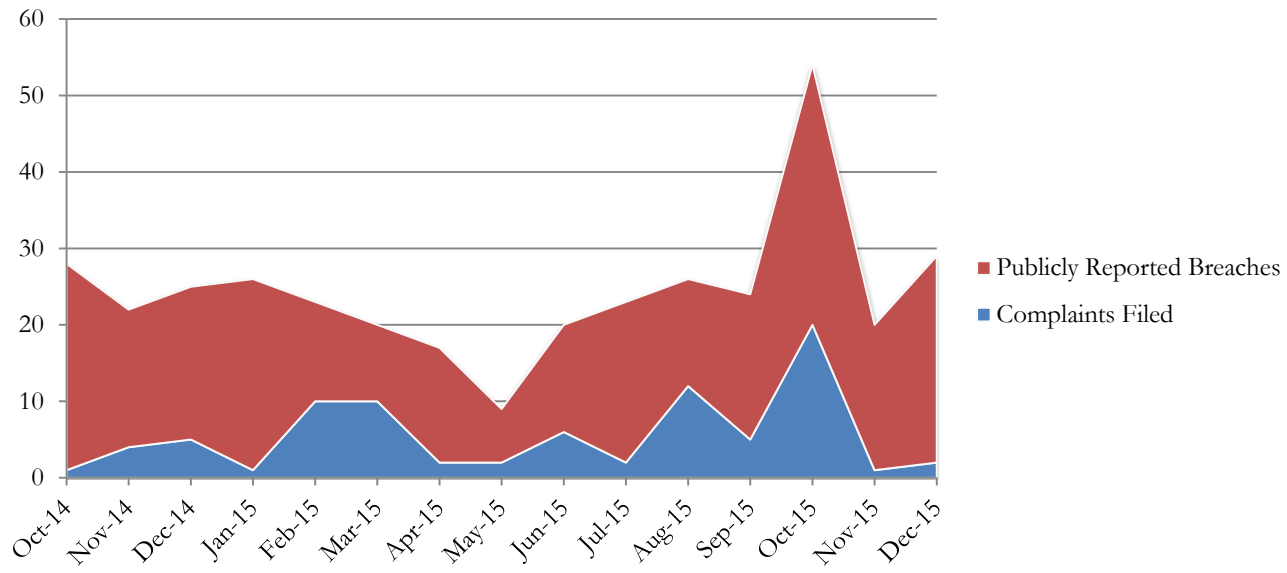
---

[4] Privacy Rights Clearinghouse estimates that in the Period, 68 of the 282 publicly reported breaches involved the medical industry. *See* http://www.PrivacyRights.org (last viewed March 22, 2016).

Part 1: Volume of Litigation

A total of 83 complaints were filed during the Period, down 24.5% from the 2015 Report.[5] This is likely the result of fewer breaches affecting the retail industry. In addition, the quantity of litigation loosely correlates with the number of publicly reported breaches in a month. For example, of the months studied in the Period, the highest number of publicly reported data breaches was reported in October 2015. Notably, the greatest percentage of complaints was filed in October 2015 (12%).[6] This can likely be explained by a spike in complaints naming Experian Information Solutions, which publicly reported a breach in the beginning of October 2015. Overall, the data shows an increase in filings naming a particular defendant 30-45 days after a company publicly reports a breach.

According to the Privacy Rights Clearinghouse Chronology of Data Breaches, 282 breaches were publicly reported during the Period.[7] However, only 83 federal class action complaints were filed during the same timeframe, and these filings related to only 21 unique defendants. As a result, slightly under 5% of publicly reported breaches ultimately led to class action litigation. This is consistent with the rate of data breach litigation identified in the 2015 Report, as well as the rate of data breach litigation identified by other studies during earlier time periods (2006 and 2010). 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.[8] This is also consistent with the estimated rate of complaint filings observed in other legal areas, including personal injury or loss.[9] The following charts provide a breakdown of class action complaints filed with the quantity of publicly reported breaches disclosed during the Period:



5 The 2015 Data Security Report is available at: http://bryancavedatamatters.com/category/white-papers/white-papers-security/.

6 *See* Privacy Rights Clearinghouse Chronology of Breaches *available at* http://www.privacyrights.org (last viewed March 22, 2016).

7 *Id.*

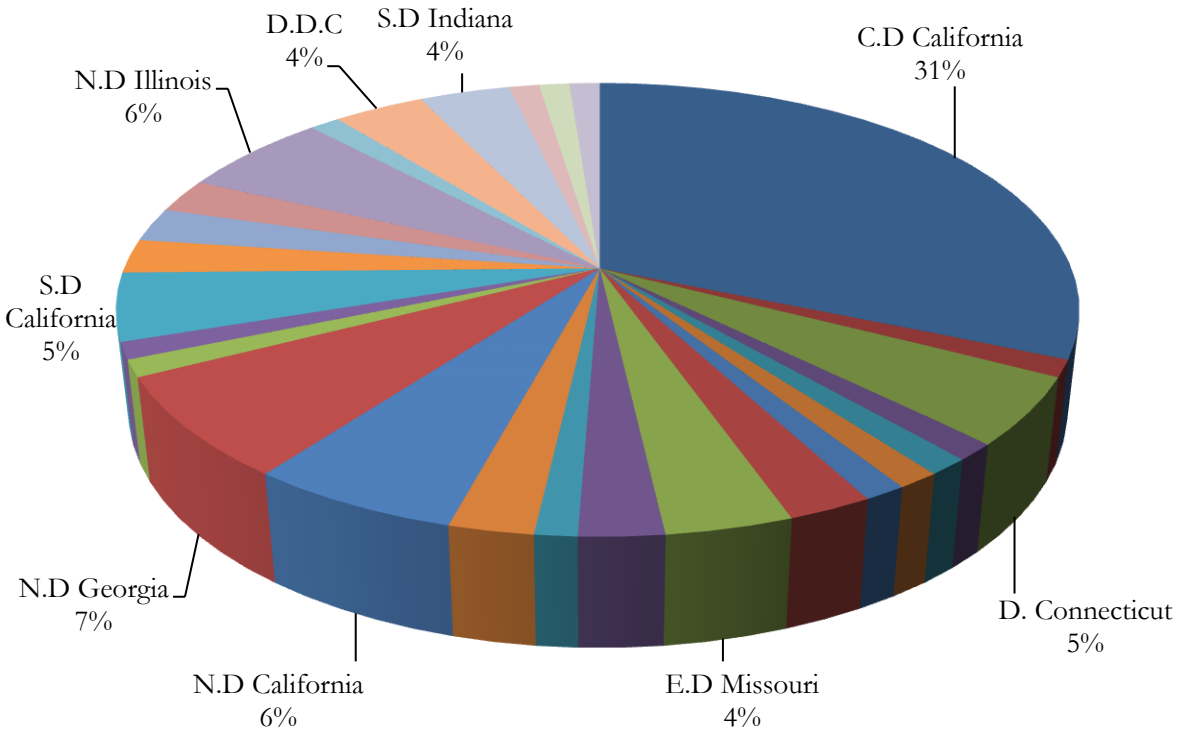
8 *See* Sasha Romanosky, *et al.,* Empirical Analysis of Data Breach Litigation, (April 6, 2013) at 10-11 *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1986461&download=yes (last viewed March 22, 2016).

9 *Id.*

Part 2: Favored Courts[10]

The Central District of California appears to be the preferred forum for filing data breach class action litigation, with almost a third of all filings originating in this jurisdiction. However, the high rate may be directly related to multiple class action filings naming Experian and Sony and alleging that the companies are headquartered in California. While Premera and Anthem also had significant complaints filed against them, no particular forum emerged as a preference. This is likely due to the fact that many complaints either named individual Anthem entities as defendants (*e.g.*, there were several complaints brought in the District of Connecticut naming Anthem Connecticut as the defendant) or alleged that Anthem conducted sufficient business in the state such that the jurisdiction was proper.

The following chart provides a detailed breakdown by district of federal class action filings:[11]



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

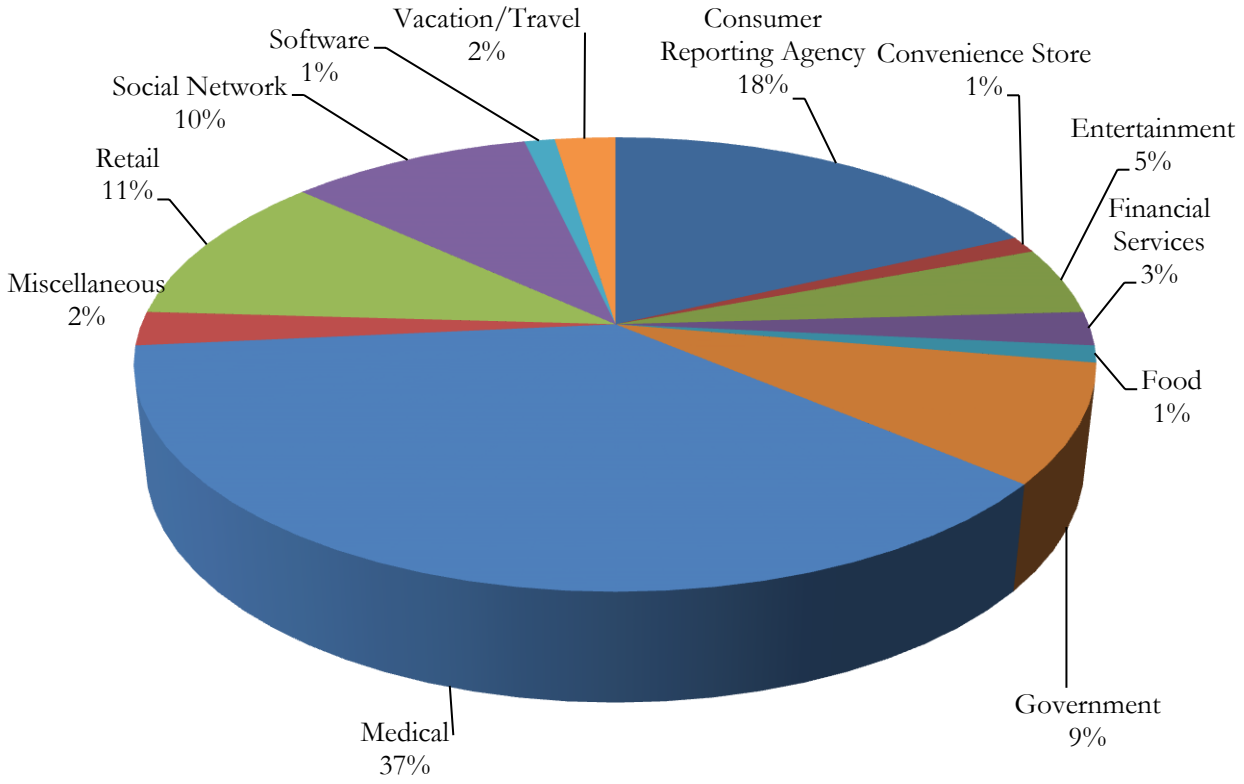
[11] The following courts are not labeled in the chart and each represent 2% of the total filings during the Period: Northern District of Alabama, Southern District of Illinois, Southern District of New York, Western District of New York, the District of Oregon, and Eastern District of Pennsylvania. The following courts are not labeled in the chart and each represent 1% of the total filings for the Period: Eastern District of California, District of Colorado, Sothern District of Florida, Northern District of Indiana, District of Kansas, Eastern District of Louisiana, District of Maine, District of Maryland, District of Minnesota, District of Ohio, Northern District of Texas, and Eastern District of Virginia.

Part 3: Litigation by Industry

The medical industry was the target of the majority of class action complaints (37%), with 31 complaints filed during the Period, a 33% increase from the 2015 Report findings. The retail industry saw only 11% of complaints, down 53% from the 2015 Report.

The second hardest hit industry, Consumer Reporting Agencies, saw a major increase due to several class action complaints naming Experian Information Solutions. The Social Network Industry also emerged as a target of class action complaints, with eight class actions filed against the owners of a dating website. The public sector also received a significant, albeit minority, of class action complaints, with the widely publicized breaches of the Internal Revenue Service and the United States Office of Personnel Management. Other industry sectors were largely ignored by plaintiffs' attorneys.

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

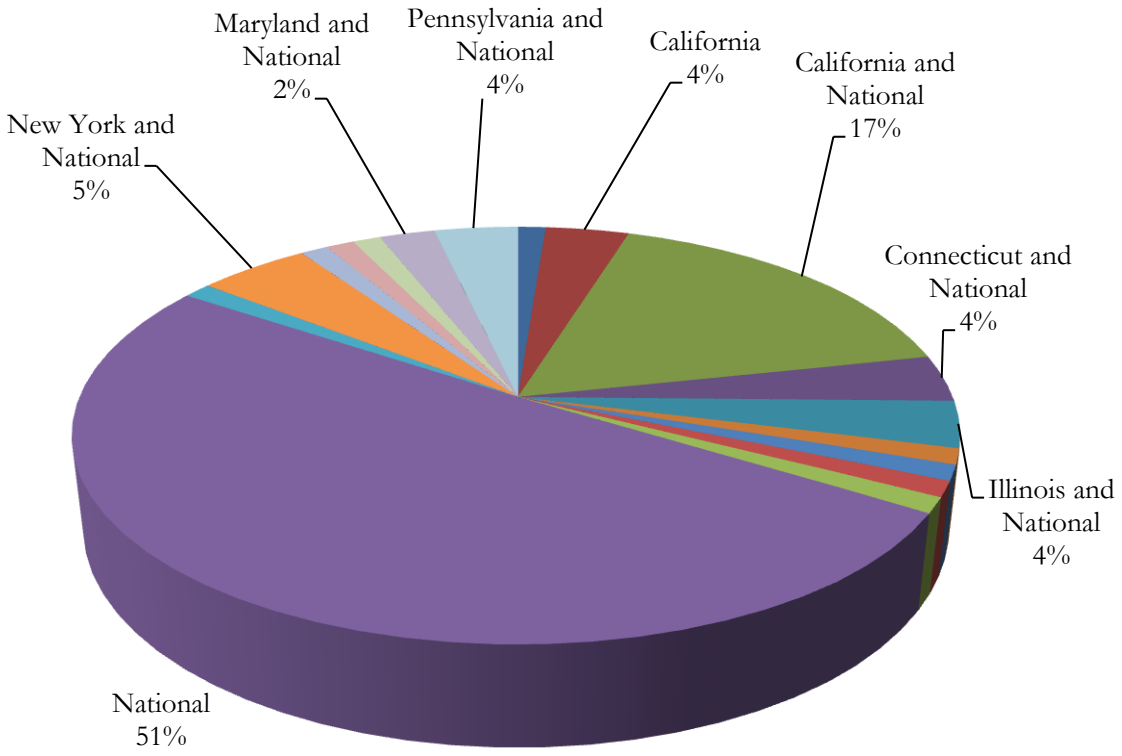


Part 4: Scope of Alleged Class (National v. State)

Access to class action complaints filed in state court differs among states and, sometimes, among courts within the same state. As a result, it is 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").

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 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 see almost half of complaints allege sub-classes tied to residents in specific states, a significant increase from the 2015 Report.[12] The following provides a detailed breakdown of the scope of putative classes:[13]



12 The 2015 Data Security Report found that only 19% of complaints alleged a subclass.

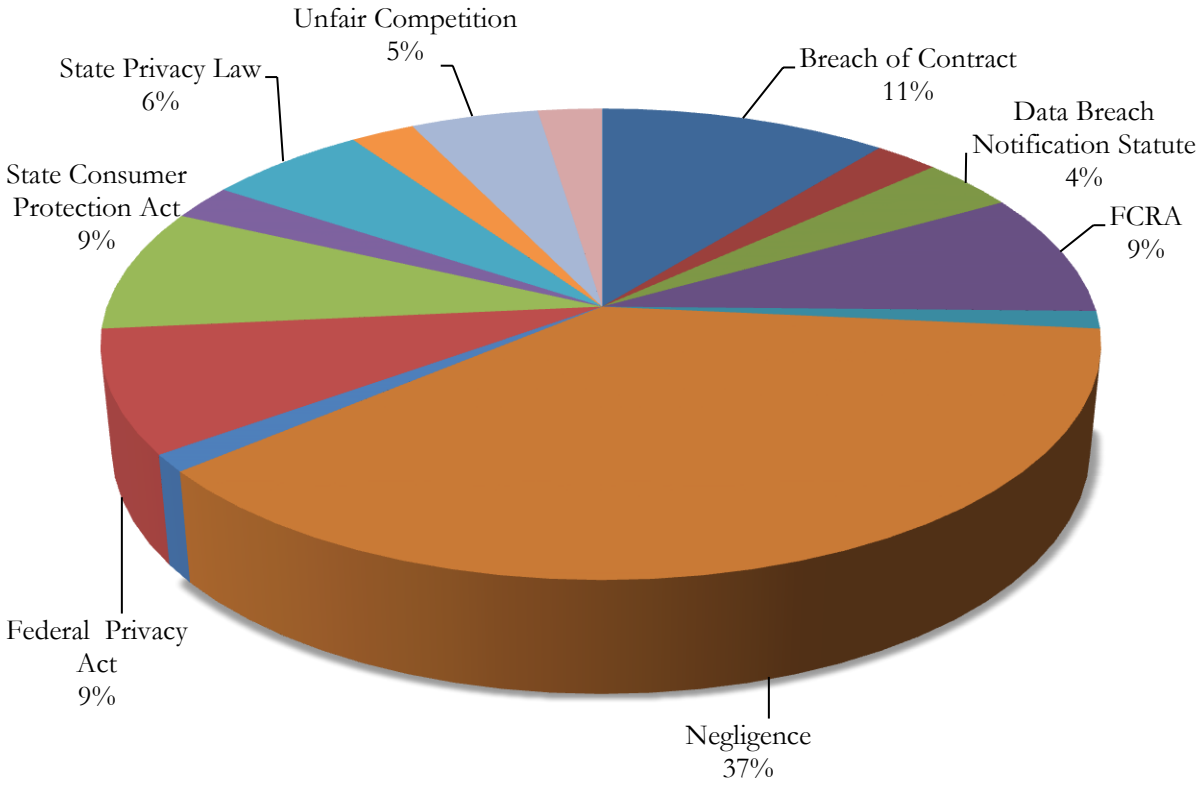
13 The following scopes of putative classes are not labeled in the chart and each represent 1% of the total filings for the Period: Missouri, Maryland, Oregon, Maine and National, Alabama and National, Kentucky and National, New Jersey and National, Ohio and National and Wisconsin and National.

Part 5: Primary Legal Theories

While regulators rely on state data breach notification laws to bring civil investigative demands and enforcement actions, these statutes are less prevalent in the context of class action lawsuits. Violation of data breach notification statutes was not the primary legal theory (the first count alleged in a complaint), with just 4% of plaintiffs alleging a violation of a data breach notification law as their first count. In addition, while plaintiffs continue to allege that companies failed to timely notify impacted consumers of a data breach, as a factual matter, most cases relate to breaches that were, in fact, announced by a company shortly after the company identified the breach.

There is no shortage of alternative theories upon which plaintiffs have brought suit. The predominant theory used by plaintiffs, however, is negligence. Although negligence was the most popular primary theory in the 2015 Report, its predominance has increased more than 14 percentage points so that now more than one third of all class action litigation alleges negligence as the primary theory of recovery.

The following chart provides a detailed breakdown of the primary theory alleged in data breach litigation complaints:[14]



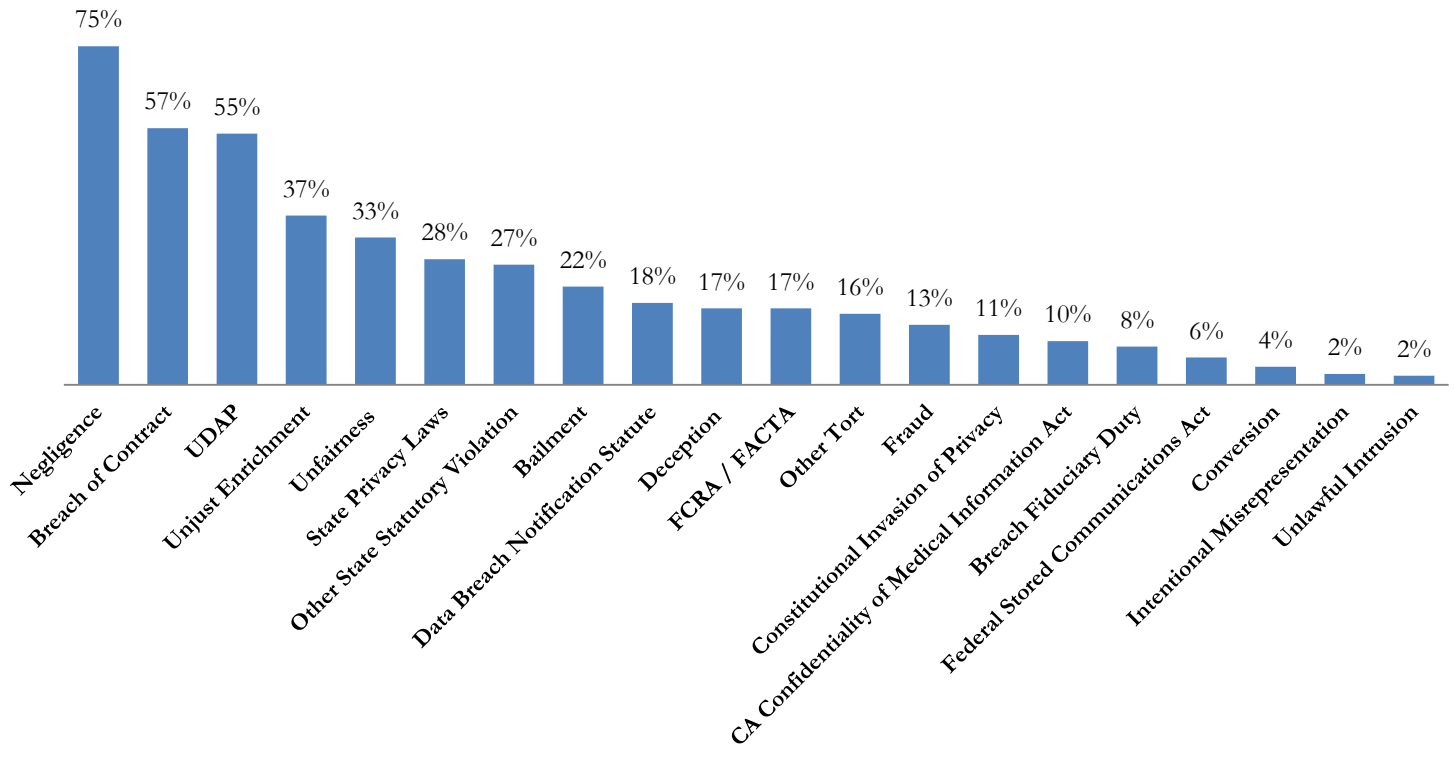
[14] The following are not labeled in the above chart and each represent 2% of primary legal theories: Unjust Enrichment, Violation of the Federal Stored Communications Act, State Consumer Record's Acts and the California Confidentiality of Medical Information Act. In addition, the following are not labeled in the chart and each represent 1% of primary legal theories: Fraud and Negligent Misrepresentation.

Part 6: Variety of Legal Theories Alleged

As discussed in Part 5, negligence was the leading "primary" legal theory used by plaintiffs' attorneys. 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 20 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 new, and popular, theory and was alleged in 21% of complaints. This can likely be explained by the spike in data breaches involving highly sensitive personal information that was entrusted to a company and the decline in breaches involving credit card information, where this theory would have little application.

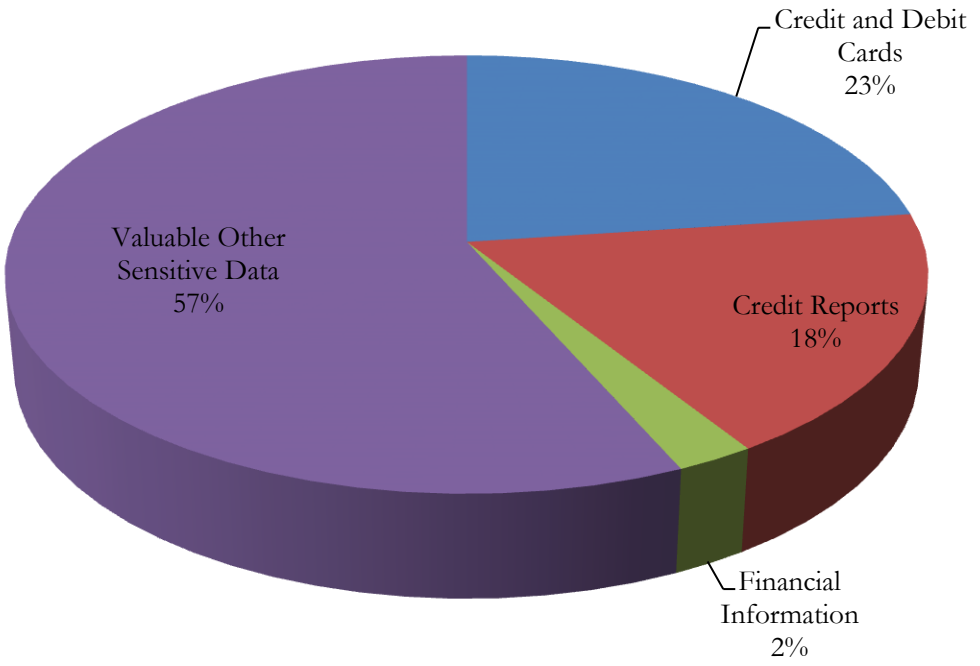
The following chart provides a detailed breakdown of all of the theories utilized by plaintiffs' attorneys in data breach litigation complaints:



Part 7: Primary Type of Data at Issue

In the 2015 Report, plaintiffs' attorneys overwhelmingly focused their resources on breaches that involved credit card numbers. That focus has decreased significantly. The quantity of class actions relating to credit cards has declined by 50 percentage points from 73% to 23%. The decrease in credit card breach class actions 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 the 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.[15] 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:



[15] *See* FTC Information Sheet, Lost or Stolen Credit, ATM, and Debit Cards *available at* http://www.consumer.ftc.gov (last viewed April 9, 2015).

Part 8: Plaintiffs' Firms

More than 65 plaintiffs' firms participated in filing class action complaints related to data security breaches. Although one plaintiffs' firm filed five 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.[16]

Data was obtained from the Westlaw Pleadings, Westlaw Dockets, and PACER databases. The sample Period covered the end of the third quarter of 2014 through the end of the third quarter of 2015 (*i.e.*, October 1, 2014-December 31, 2015). 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.*, "Anthem" and "breach") not all of the complaints filed as a result of these data breaches were found using Westlaw (*i.e.*, our search results produced around 31 complaints, while some sources suggest that more than 100 lawsuits were filed against Anthem).[17] The 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.

---

16 As referenced above, the 2016 study differs from the 2015 Report in that it includes complaints filed against government agencies.

17 *See MDL Established for Anthem Data Breach Class Actions* http://legalnewsline.com/stories/510550820-mdl-established-for-anthem-data-breach-class-actions.

AUTHORS

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.

Bryan Cave LLP
Boulder, CO / Washington D.C.
David.Zetoony@bryancave.com
202-508-6030

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.

Bryan Cave LLP
Chicago, IL
Jena.Valdetero@bryancave.com
312-602-5056

Joy Anderson is an associate in Bryan Cave's Commercial Litigation Client Service Group and a member of the firm's Data Privacy and Security Team

Bryan Cave LLP
Chicago, IL
Joy.Anderson@bryancave.com
312-602-5147

Bryan Cave LLP

Bryan Cave is a leading international law firm with offices in 24 cities and 12 countries. The firm routinely defends clients in private litigation and regulatory enforcement actions involving data security breaches, and has assisted in over 500 data security incidents and breaches.

If you would like to receive information about future data privacy and security publications you can register for Bryan Cave's distribution list at http://www.bryancavedatamatters.com.

Any questions or comments concerning this report, or requests for permission to quote, or reuse it, should be addressed to the authors above.