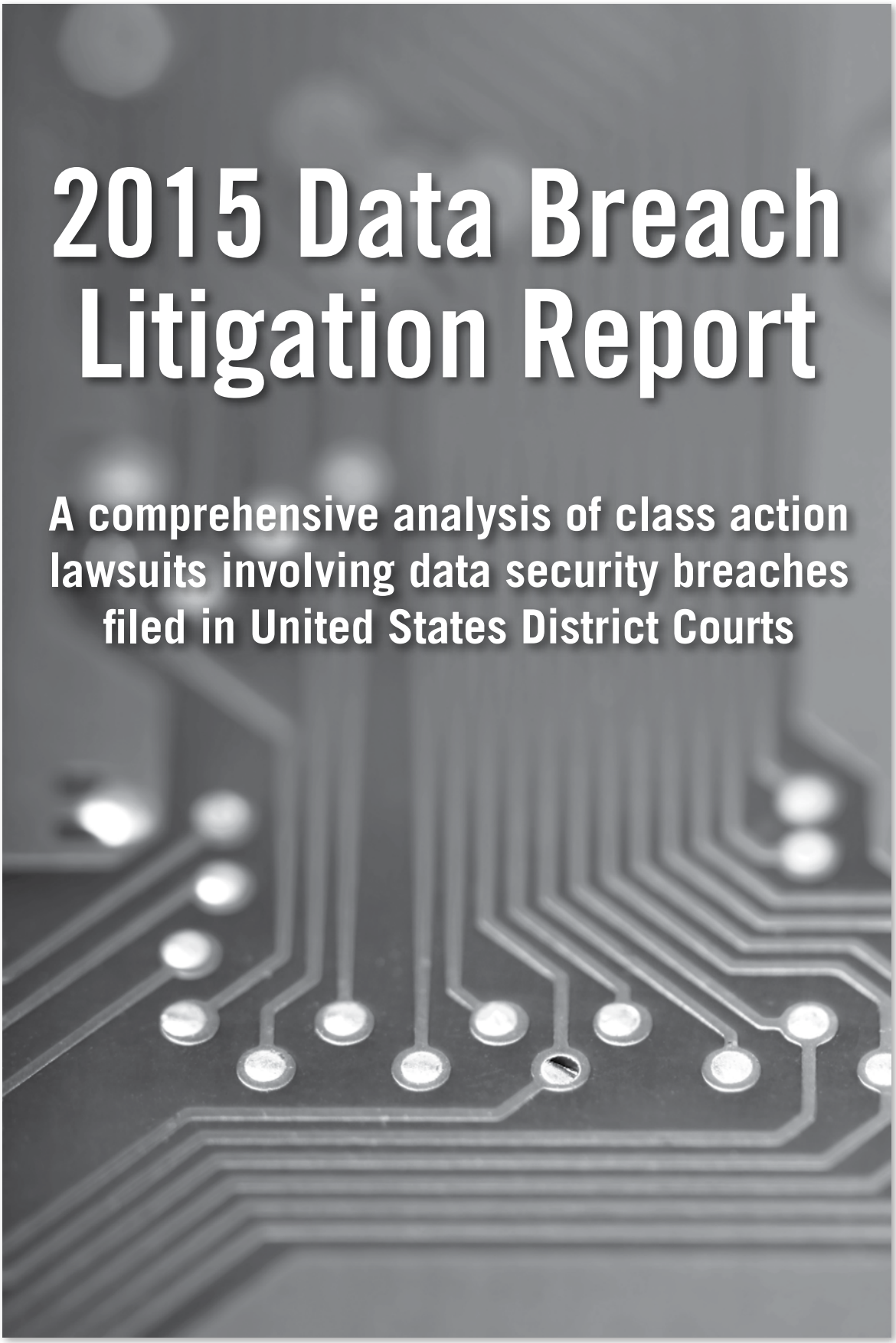


2015 Data Breach Litigation Report

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

By David Zetoony,* Josh James,** Leila Knox, ***
Tracy Talbot, **** and Amber Williams*****

Executive Summary

Data security breaches – and data security breach litigation – dominated the headlines in 2014 and continue to do so in 2015. Indeed, over 31,000 articles now reference data breach litigation.[1]

While General Counsel cite class action fears as one of their top concerns following a data breach, there is a great deal of misunderstanding concerning the nature of data security breach class action litigation. A main cause of that misunderstanding has been a lack of reliable statistics. Two years ago Bryan Cave's Data Privacy and Security Team set out to rectify the information gap by publishing what has become the most comprehensive survey and analysis of consumer class action complaints relating to data security breaches.

Our 2015 report covers litigation initiated over a 15 month period from the third quarter of 2013 through the third quarter of 2014 (the "Period"). Our key findings are:

- The overall volume of class action filings was significantly less than what was implied in the media. Approximately 110 cases were filed during the Period.
- When multiple filings against single defendants are removed, there were only 25 unique defendants during the Period. This evidences a "lightening rod" effect by plaintiff's attorneys to file multiple cases against companies connected to the largest and most publicized breaches; the vast majority of other companies that experienced a data breach were ignored by the plaintiffs' bar.
- Approximately 4% of publicly reported data breaches led to class action litigation.
- The Northern District of Illinois and the Northern District of California emerged as preferred forums for plaintiffs. The District of Minnesota and the Northern District of Georgia were also popular courts during the Period, this popularity was primarily due to their status as the home forums for two companies involved with the largest breaches during the Period.
- The retail industry has been disproportionately targeted by the plaintiff's bar. While only 14.5% of publicly reported breaches related to the retail industry, nearly 80% of class actions targeted retailers.[2]
- While plaintiff's attorneys alleged 24 different legal theories, there is a growing bias toward negligence and contract oriented theories.
- Plaintiff's attorneys have overwhelmingly focused on credit card breaches to the exclusion of breaches involving arguably more sensitive consumer information (*e.g.,* Social Security Numbers).

Part 1: Volume of Litigation

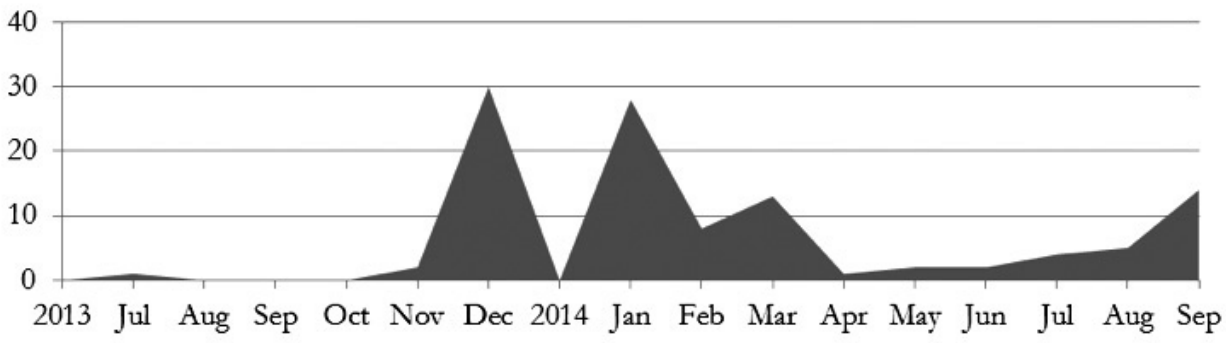
While a total of 110 complaints were filed during the Period, there was significant variation on a month-to-month basis. In addition, the quantity of litigation does not correlate with the number of publicly reported breaches in a month. For example, according to one interest group that tracks publicly reported breaches, nearly the same quantity of breaches were reported in January of 2014 as in April of 2014. However, twenty times more class action complaints were filed in January as compared to April.[3]

The volume discrepancy is due primarily to multiple class action complaints filed in connection with two large-scale credit card breaches that received significant media attention. Specifically, the vast majority of complaints filed in December of 2013 and January of 2014 related to the widely publicized Target data breach. Similarly, the majority of complaints filed in September of 2014 related to the highly publicized data breach of Home Depot.

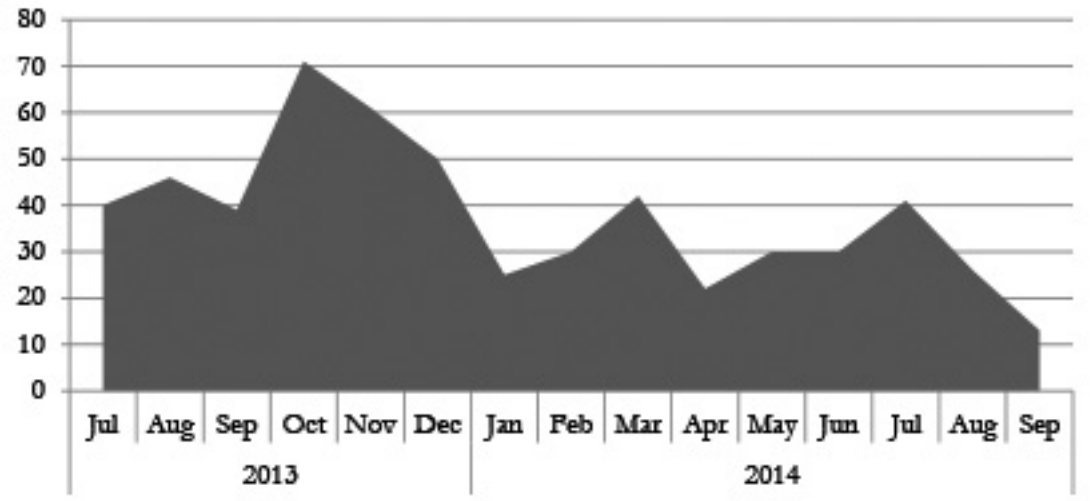
According to the Privacy Rights Clearinghouse Chronology of Data Breaches, 566 breaches were publicly reported during the Period.[4] However, only 110 federal class action complaints were filed during the same time frame and these filings related to only 25 unique defendants. As a result, slightly over 4% of publicly reported breaches ultimately led to class action litigation. This is consistent with the conclusion of other studies that found a similar rate of data security breach litigation between 2006 and 2010, and suggests that there has not been an increase in the rate of complaint filings when total complaints are normalized by the quantity of breaches.[5] This is also consistent with the estimated rate of complaint filings observed in other legal areas, including personal injury or loss.[6]

The following charts provide a breakdown of class action complaints filed with the quantity of publicly reported breaches disclosed during the Period: (See chart below and on page 92)

Class Action Complaint Filings



Publicly Reported Data Breaches

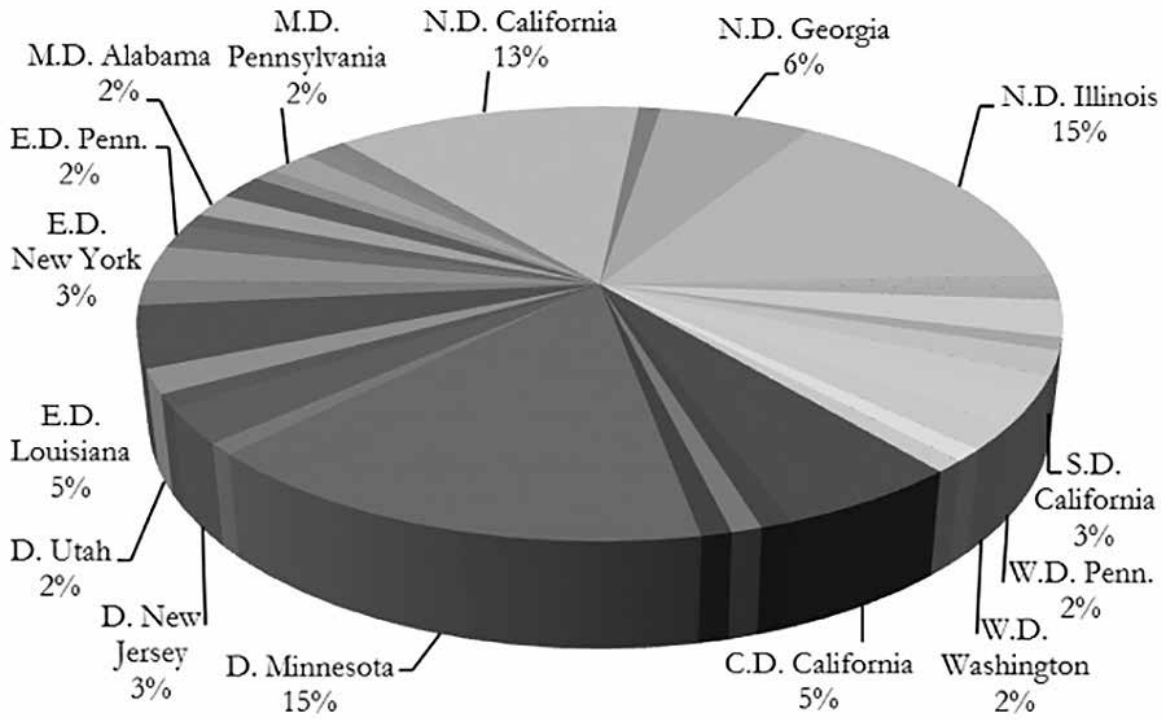


Part 2: Favored Courts[7]

Plaintiffs have demonstrated a clear preference for bringing data breach litigation in certain forums – specifically, the Northern District of Illinois and the Northern District of California. The preference may be due, in part, to a perception of those forums as being plaintiff friendly.

An equally popular, but perhaps less expected, forum was the District of Minnesota and, to a lesser extent, the Northern District of Georgia. The high rate of filing in both of these forums, however, was directly related to multiple class action filings against Target, which is located in Minnesota, and Home Depot, which is located in Georgia. If litigation relating to these two breaches is removed from the dataset, there does not appear to be any plaintiff preference for either forum.

The following chart provides a detailed breakdown by district of federal class action filings:[8]

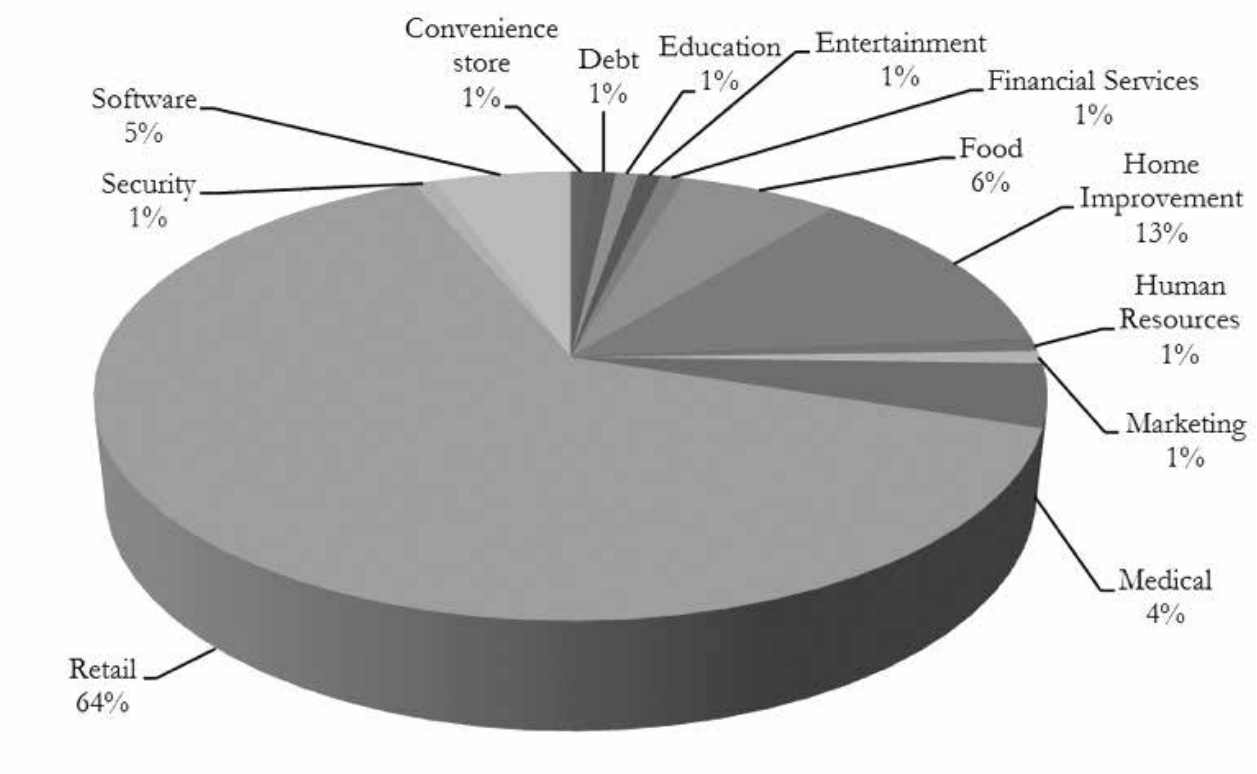


Part 3: Litigation by Industry

The retail industry was the target of the vast majority of class action complaints (64%), with 70 complaints filed against retailers during the Period. Note that for the purpose of this study we have treated the home improvement industry – which would include companies such as Home Depot – and the convenience store category as separate from retail. If complaints filed against home improvement and convenience stores that sell primarily to end-use consumers are included in the general retail category, nearly 80% of all class action complaints target the retail sector.

Although the data analyzed in this report was taken prior to the widely publicized breach of Anthem, Inc., the medical industry still received a significant, albeit minority, of class action complaints. The food sector and the software sector also received a significant, albeit minority, of class action complaints. Other industry sectors were largely ignored by plaintiff's attorneys.

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

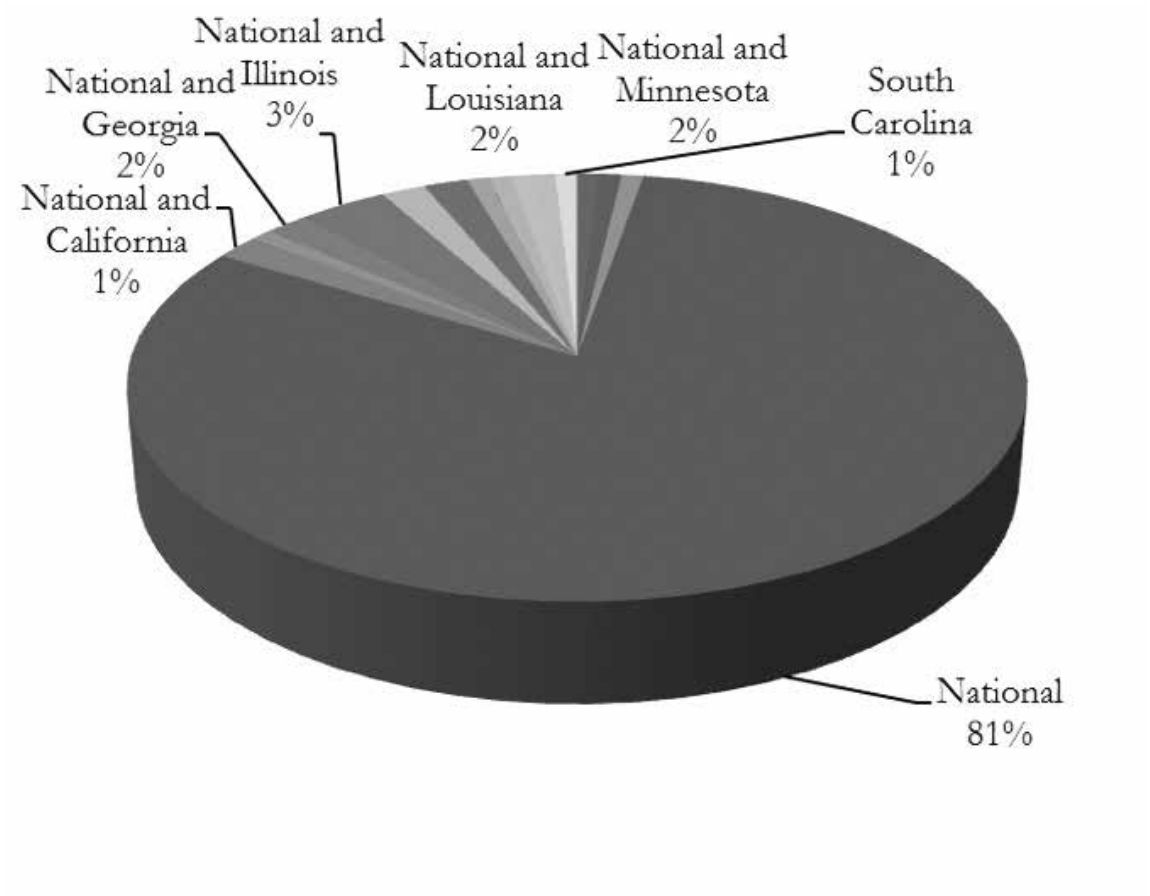


Part 4: Scope of Alleged Class (National v. State)

Access to class action complaints filed in state court differ 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 plaintiff's 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 continue to see a minority of cases (19%) allege sub-classes tied to residents in specific states. The following provides a detailed breakdown of the scope of putative classes:

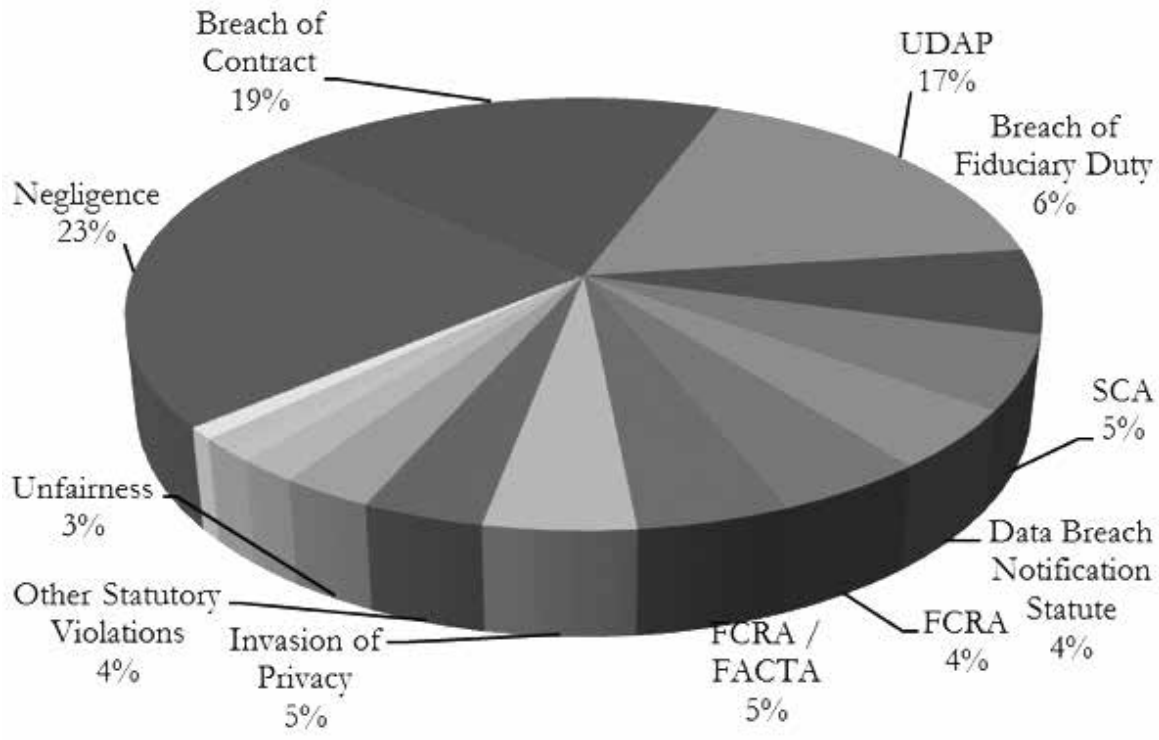


Part 5: Primary Legal Theories

The media, regulators, and Congress continue to focus their attention on state enacted "data breach notification laws." Though these statutes were not a popular primary legal theory, 40% of plaintiffs alleged a data breach notification law as a secondary theory in their complaint.[9] 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 discovery.

There is no shortage of alternative theories upon which plaintiffs have brought suit. While the predominant theory is negligence, it does not yet dominate the landscape, and the predominant theory in nearly as many suits is breach of contract. Following negligence and breach of contract, the most common statutory allegation is that alleged poor data security violated general state consumer protection or unfair or deceptive trade practice laws.

The following chart provides a detailed breakdown of the primary theory alleged in data breach litigation complaints:[10]

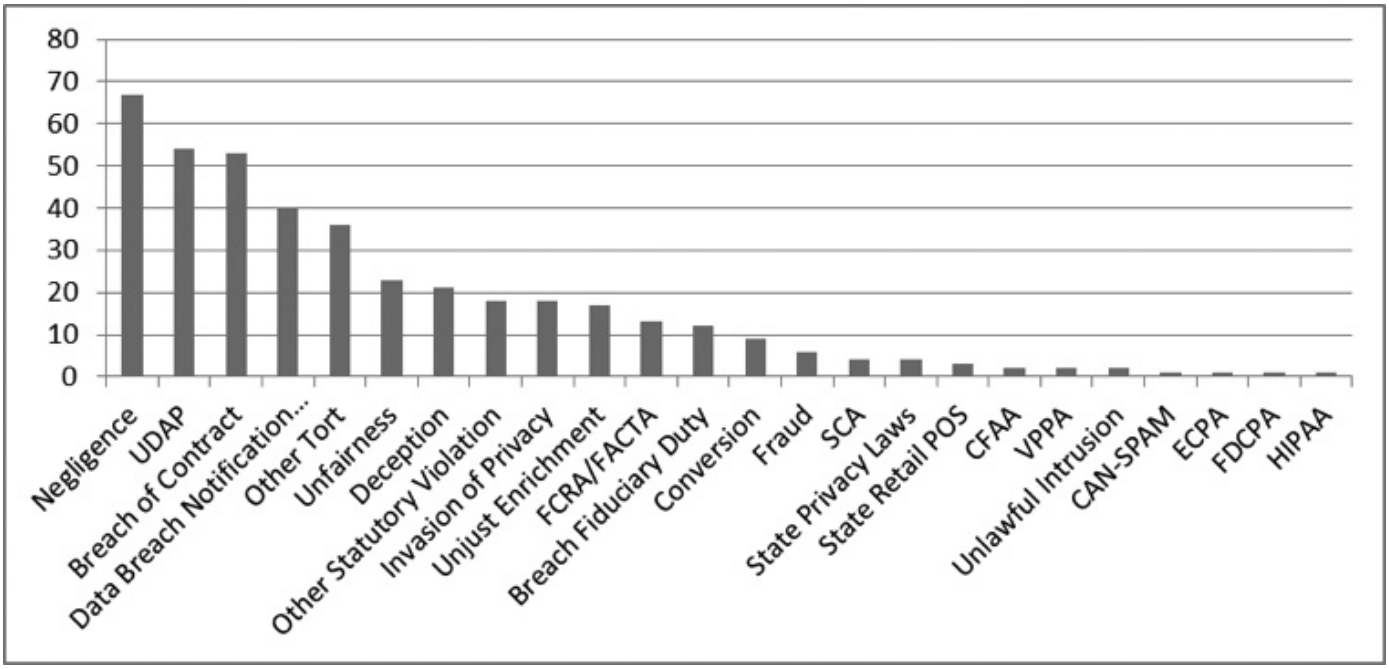


Part 6: Variety of Legal Theories Alleged

As discussed in Part 5, negligence and breach of contract were the leading "primary" legal theories used by plaintiff's attorneys. Although negligence and breach of contract may be the most common theories first put forward by a plaintiff's attorney, most plaintiffs choose to allege more than one theory of recovery, and some plaintiff's attorneys choose to include theories sounding in contract, tort, and statute.

As indicated in the table below, although plaintiff's attorneys show a clear preference for some legal theories – *e.g.,* breach of contract, negligence, and state statutes prohibiting unfair or deceptive acts and practices – in total they have pursued 24 different legal theories of recovery.

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



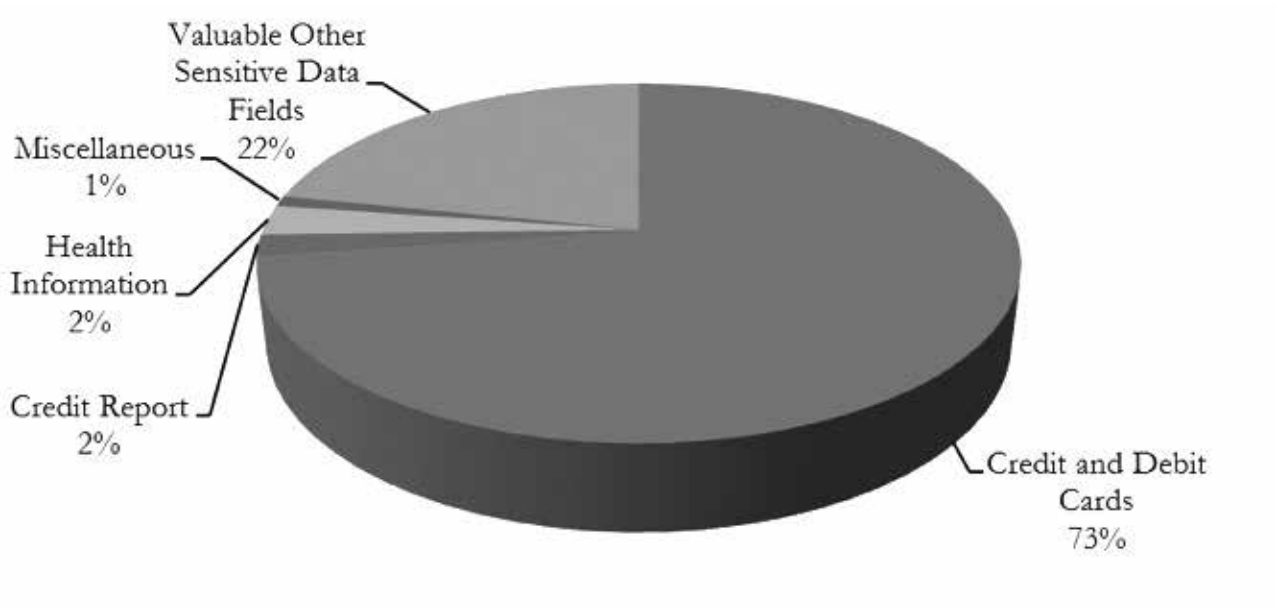
Part 7: Primary Type of Data at Issue

Privacy advocates have advanced different theories concerning what types of data are, and are not, more important to consumers if lost or stolen. While some advocates contend that the loss of a Social Security Number is the most harmful to consumers' privacy, as it can directly lead to identity theft which can cause economic injury, other privacy advocates argue that consumers care as much, if not more, about the loss of medical or salary information, as that data may result in shame or embarrassment.

Unlike other types of sensitive personal information, credit card account numbers can neither be used for identity theft (at least to the extent that the term refers to the opening of new accounts in the name of a consumer) or to embarrass or shame a consumer. While criminals that obtain a consumer's credit card may make fraudulent charges on the consumer's account, 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.[11] As a result of many banks and payment card networks now voluntarily waiving even the $50 that the consumer may be liable for under federal law, in most instances consumers suffer no financial harm as a result of a breach that involves their credit card.

Despite a lack of concrete financial harm connected with the loss of a credit card, plaintiff's attorneys continue to focus their resources overwhelmingly on breaches that involve credit card numbers.

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



Part 8: Plaintiff's Firms

Over 70 plaintiff's firms participated in filing class action complaints related to data security breaches. Although one plaintiff's firm filed seven 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 filed against government agencies, or complaints that were filed on behalf of individual plaintiffs were excluded.

Data was obtained from the Westlaw Pleadings and the Westlaw Dockets databases. The sample Period covered the beginning of the third quarter of 2013 through the end of the third quarter of 2014 (*i.e.*, July 1, 2013-September 30, 2014). 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,"
- "data" at a reasonable distance from "breach," or
- "target" and "home depot" at a reasonable distance from "breach."

Although searches were conducted using "target" and "home depot," not all of the complaints filed as a result of these data breaches were found using Westlaw (*i.e.*, our search results produced around 56 complaints, while it is general knowledge that more than 140 lawsuits were filed against Target).[12] The discrepancy may be due in part to the speed at which the multiple filings were consolidated.

Additional searches were used to identify complaints that specifically referenced the Health Insurance Portability and Accountability Act ("HIPAA"), the Video Privacy Protection Act ("VPPA"), the Fair Credit Reporting Act ("FCRA"), the Fair and Accurate Credit Transactions Act ("FACTA"), the Fair Debt Collection Practices Act ("FDCPA"), and the Electronic Communications Privacy Act ("ECPA").

All the complaints identified by these searches were read and, after the exclusion of the 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 which are removed from state court to federal court were included within the analysis.

* David Zetoony is the leader of consumer protection group. David's practice focuses on advertising, data privacy, and data security and he is the Chair of the firm's Global Data Privacy and Security Team. Bryan Cave LLP, Boulder, CO / Washington D.C.] David.Zetoony@bryancave.com, 202-508-6030.

** Josh James is a member of Bryan Cave's Data Privacy and Security Team and routinely assists clients in responding to data security breaches and in investigations initiated by the Federal Trade Commission.

Bryan Cave LLP, Washington D.C., Josh.James@bryancave.com, 202-508-6265. Other Bryan Cave White Papers may be found at http://www.bryancavedatamatters.com.

*** Leila Knox focuses her practice on the area of specializing in media law and intellectual property. Bryan Cave LLP, San Francisco, CA, Leila.Knox@bryancave.com, 415-268-1949.

****Tracy Talbot focuses her practice in the area of commercial and intellectual property litigation. Bryan Cave LLP, San Francisco, CA, Tracy.Talbot@bryancave.com, 415-675-3442.

***** Amber Williams obtained a JD from the University of Colorado Law School, Boulder, CO in May 2015 and served as the 2015 privacy intern for the Bryan Cave Data Privacy and Security Team.

---

1 Google News Search for "Data Breach Litigation" conducted on April 9, 2015.

2 Privacy Rights Clearinghouse estimates that in 2014, 43 of the 295 publicly reported breaches involved retailers. *See* http://www.PrivacyRights.org (last viewed April 9, 2015).

3 According to Privacy Rights Clearinghouse Chronology of Data Breaches, 25 breaches were publicly reported in January of 2014, compared to 23 in April of 2014. *See* Privacy Rights Clearinghouse Chronology of Breaches *available at* http://www.privacyrights.org (last viewed April 9, 2015).

4 *See* Privacy Rights Clearinghouse Chronology of Breaches *available at* http://www.privacyrights.org (last viewed April 9, 2015).

5 *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 May 7, 2015).

6 *Id.*

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

8 The following courts are not labeled in the chart and each represent 1% of the total filings for the Period: Middle District of Alabama; Northern District of Alabama; District of Colorado; Northern District of Florida; Southern District of Florida; District of Kansas; District of Massachusetts; District of New Hampshire; Northern District of New Jersey; Southern District of New York; Middle District of North Carolina; Northern District of Ohio; District of Rhode Island; Middle District of Tennessee; and the Western District of Wisconsin. In addition, the following courts are not labeled in the chart and each represent 2% of the total filings during the Period: Eastern District of Missouri; Middle District of Florida; and the Southern District of Illinois.

9 Please see Part 6 for additional information.

10 Additionally, 2% of plaintiffs claimed the VPPA as their primary legal theory. Fraud, HIPAA, and Unjust Enrichment each represented 1% of plaintiffs' primary legal theories during the Period.

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

12 *See* Target Breach Lawsuits Consolidated: Banking Suits Seek Recovery of Expenses *available at* http://www.bankinfosecurity.com/target-breach-lawsuits-consolidated-a-6845/op-1 (last viewed April 14, 2015).