# 2015 Data Privacy Litigation Report

A comprehensive analysis of class action lawsuits involving data privacy issues filed in the United States District Courts.

BRYAN CAVE

**Executive Summary**

Litigation related to data privacy (*i.e.*, the collection, use, and sharing of information) receives less attention from the media and the legal press than litigation related to data security and, specifically, to data breaches. As discussed in this Report, however, there is far more litigation centered on data privacy than on data breaches. Indeed, plaintiff's attorneys are six times more likely to file a complaint relating to an event concerning data privacy than one concerning a data breach. In addition, three times more plaintiff's law firms have invested resources in bringing data privacy cases than have invested resources in data security breach litigation.

Our 2015 Report includes 15 months of data, covering the third quarter of 2013 through the third quarter of 2014 (the "Period"). Our key findings are:

- Over 600% more data privacy complaints were filed than data security breach complaints during the same Period.

- Approximately 672 data privacy complaints were filed during the Period.

- Nearly one third of all data privacy litigation is filed in California federal courts. Plaintiff's attorneys have expressed a strong preference specifically for the United States District Court for the Central District of California. In contrast, plaintiff's attorneys prefer the United States District Court for the Northern District of California for data breach litigation.

- The volume of data privacy complaints rose each quarter.

- The majority of data privacy litigation (65%) relates to telemarketing and the Telephone Consumer Protection Act.

- Relatively little data privacy litigation (1%) relates to point of sale collection statutes, despite the wide coverage those statutes have received in the legal media.

- Data privacy litigation crosses almost every industry sector, although the financial service industries (*i.e.*, traditional financial services, loan providers, insurance companies, credit cards, and debt collectors) account for nearly half (46%) of all complaints.

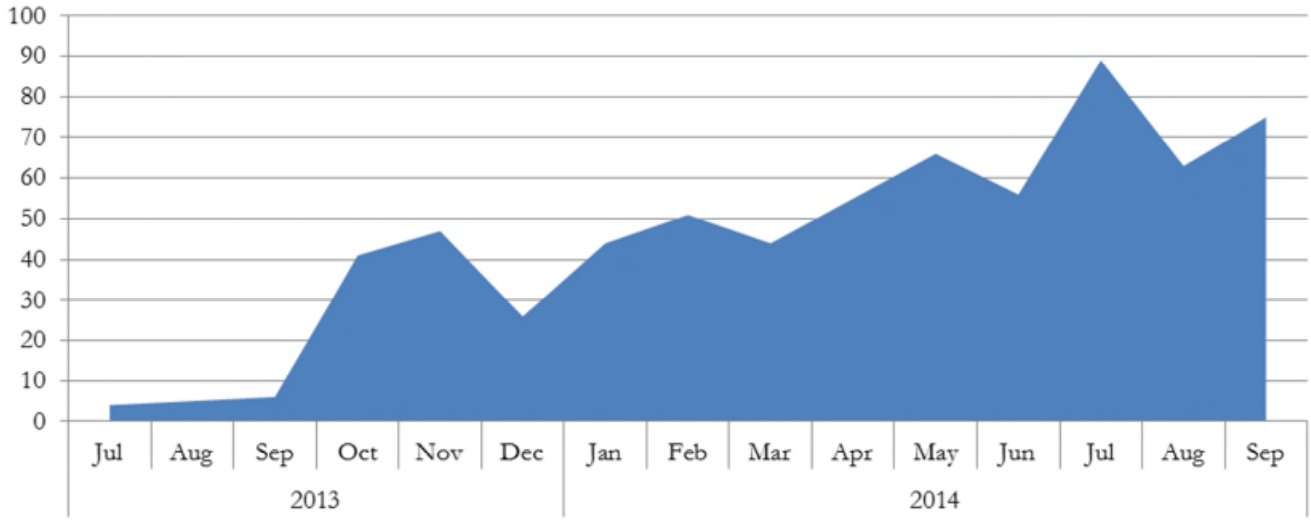
- 1.5% of plaintiff's firms that are active in data privacy litigation account for nearly one third of all data privacy litigation filings.

## Part 1: Volume of Litigation

A total of 672 complaints involving data privacy were filed during the Period. Complaint filings increased each quarter during the period, and suggest an ongoing upward trend.

The volume of data privacy litigation is significantly greater than the volume of data security breach litigation, which has received more attention from the legal and popular press. Indeed, there were 600% more data privacy complaints filed during the Period than data security complaints.[1] On a month-to-month basis the volume of data privacy complaints was also more consistent. Whereas two thirds of data breach cases were filed during three months of the Period (December of 2014, and January and September of 2015), more than 30 data privacy complaints were filed each month over a span of eleven months during the Period.

The following chart provides a breakdown of class action complaints involving data privacy during the Period:

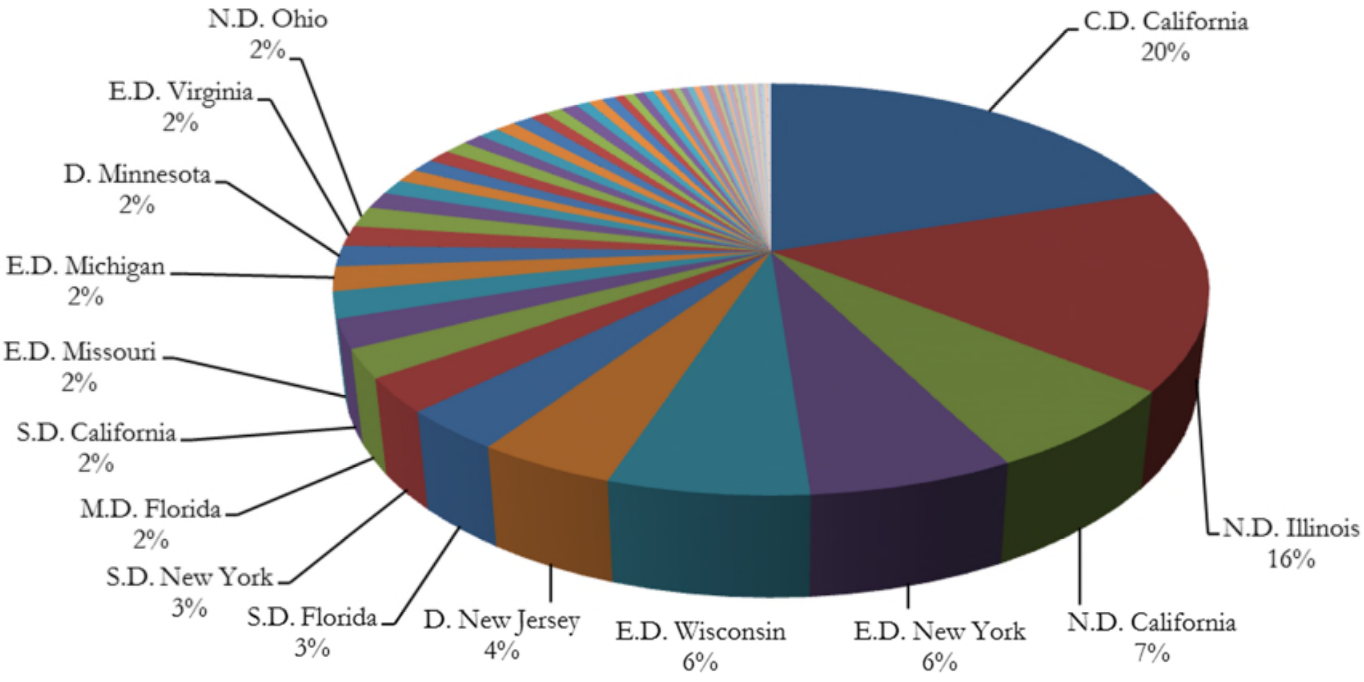



[1] *See* Bryan Cave, 2015 Data Breach Litigation Report (May 2015) *available at* http://www.bryancavedatamatters.com (the "Data Breach Litigation Report"). The Data Breach Litigation Report identified a total of 110 complaints concerning data breaches filed during the same Period.

## Part 2: Favored Courts[2]

California remained the most popular venue for privacy complaints – nearly 30% of all complaints were filed in California federal district courts.[3] While California's popularity among plaintiffs may be due in part to consumer-friendly privacy laws specific to California (*e.g.*, the Song-Beverly Act), the majority of cases filed in California were not based on privacy legislation unique to the state. Plaintiffs preference for California federal district courts is more likely a result of the fact that some (but not all) of the defendants are based or headquartered in California facilitating the personal jurisdiction of a California court, along with a general perception of California courts – and recent rulings of the Ninth Circuit – as being plaintiff friendly. Following California, the Northern District of Illinois was the second most preferred forum among plaintiffs.

The following chart provides a detailed breakdown by district of federal class action filings:[4]




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

3 *See* http://www.bryancavedatamatters.com/ for past Reports on Data Privacy Litigation.

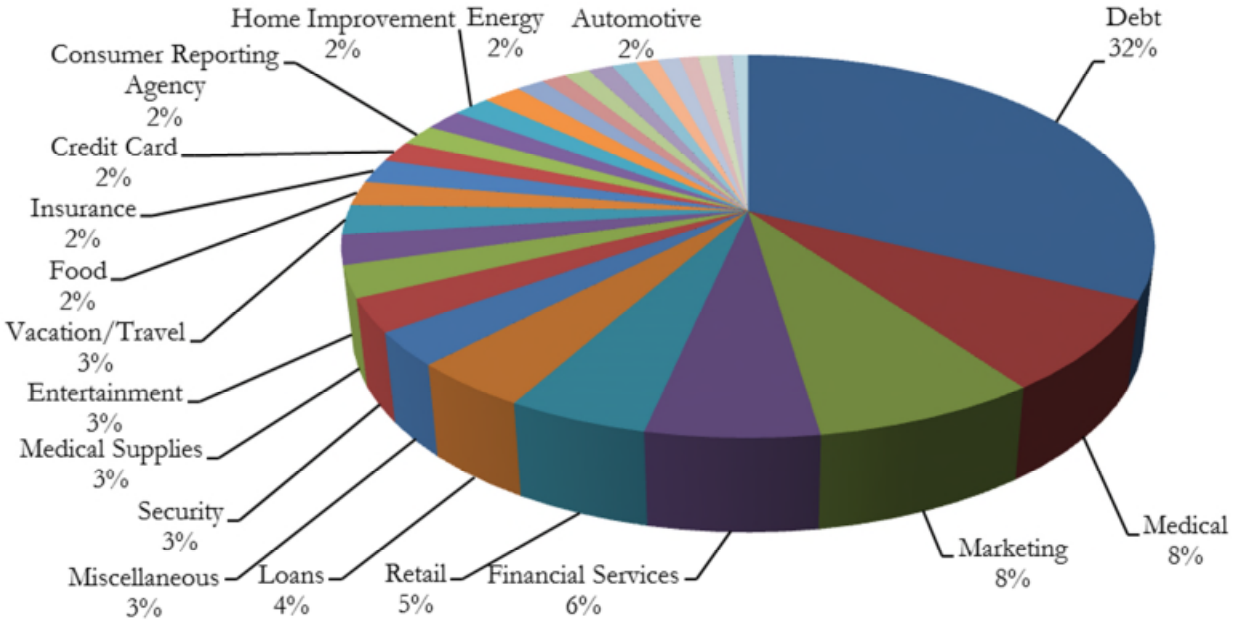
4 There are 46 additional courts that are not labeled in the chart and each represents 1% or less of the total filings during this period.

## Part 3: Litigation by Industry

Our prior Reports identified the debt collection industry as the primary industry targeted by plaintiffs.[5] That trend continued with almost a third of all data privacy-related complaints being filed against debt collectors. Although the debt collection industry received the most privacy-related complaints, no industry was spared and the remainder of complaint filings were spread across almost every sector.

Interestingly, there is a significant disparity between the industries targeted by plaintiff's attorneys in data security breach litigation and data privacy litigation. As was noted in our 2015 Data Breach Litigation Report, 80% of all data security breach complaints targeted the retail industries (*i.e.*, general retail and home improvement). In comparison, only 9% of data privacy complaints targeted the retail industries (*i.e.*, general retail, home improvement, and food).

The following chart provides a detailed breakdown of class action complaint filings by industry sector:[6]




5 Bryan Cave LLP, *Shifting Trends: Privacy & Security Class Action Litigation* (Sept. 2014) *available at* http://www.bryancavedatamatters.com (the "Second Quarter 2014 Report").

6 While not identified in the chart, the following industries each received 2% or less of the complaint filings: Transportation; Pharmaceutical; Fitness; Manufacturing; Human Resources; Social Network; Software; Apps; Telecommunications; Search Engine; and Education.

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

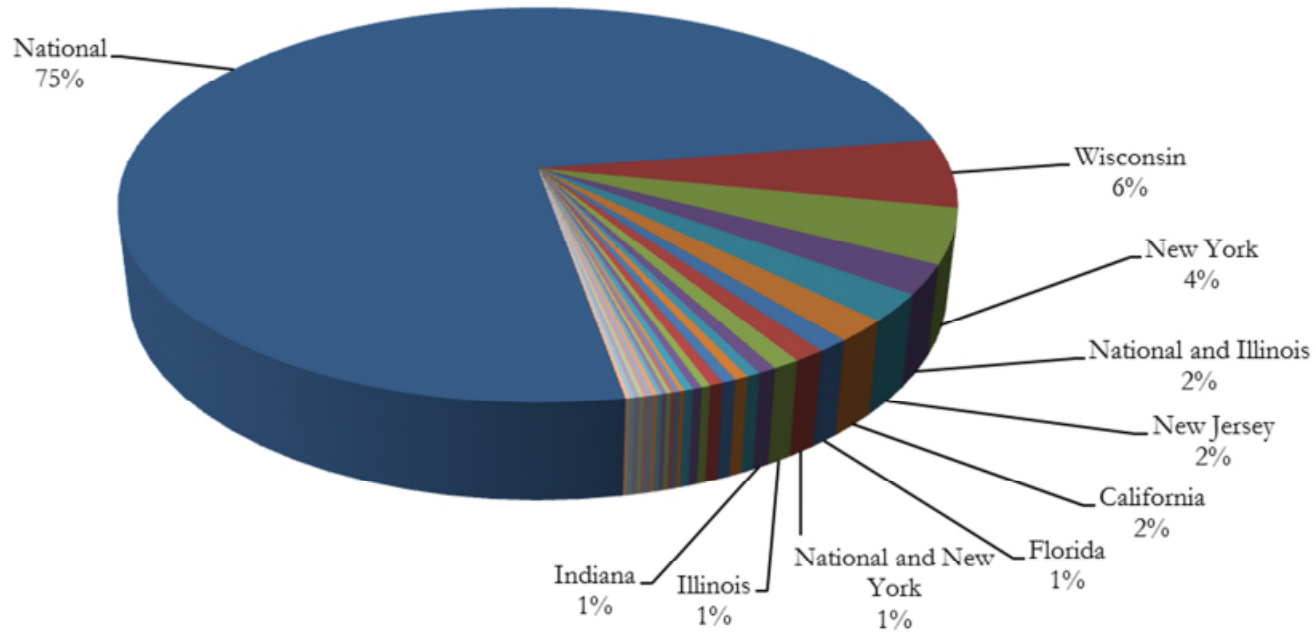
Access to class action complaints filed in state court differ among states, and sometimes, among courts within the same state. As a result, it is difficult, if not impossible, to identify the total quantity of class action filings in state courts, and any analysis that includes state court filings would include a significant and misleading skew toward states that permit easy electronic access to filing complaints. As a result, we purposefully do not include state court filings in our analysis and focus only on complaints filed in federal district court and complaints originally filed in state court that were subsequently removed to federal district 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 a potentially greater recovery, especially in TCPA cases, where thousands of consumers are typically alleged to have been contacted illegally. It could also mean, however, that additional complaints not included in our analysis were filed in state court alleging putative classes comprised of single state groups.

Despite the preponderance of national class actions, a minority of cases (17%) alleged state-only classes. A smaller minority (3%) alleged a national class as well as a state subclass.

There is a significant disparity between the distribution of putative national classes in data privacy litigation compared to the quantity of putative national classes in data security litigation. Although in both categories the majority of cases allege a putative national class, as our 2015 Data Breach Litigation Report indicates, there is a far greater emphasis on national classes in the data breach context (91%) as compared to the data privacy context (75%).

The following chart provides a detailed breakdown of the scope of putative classes:



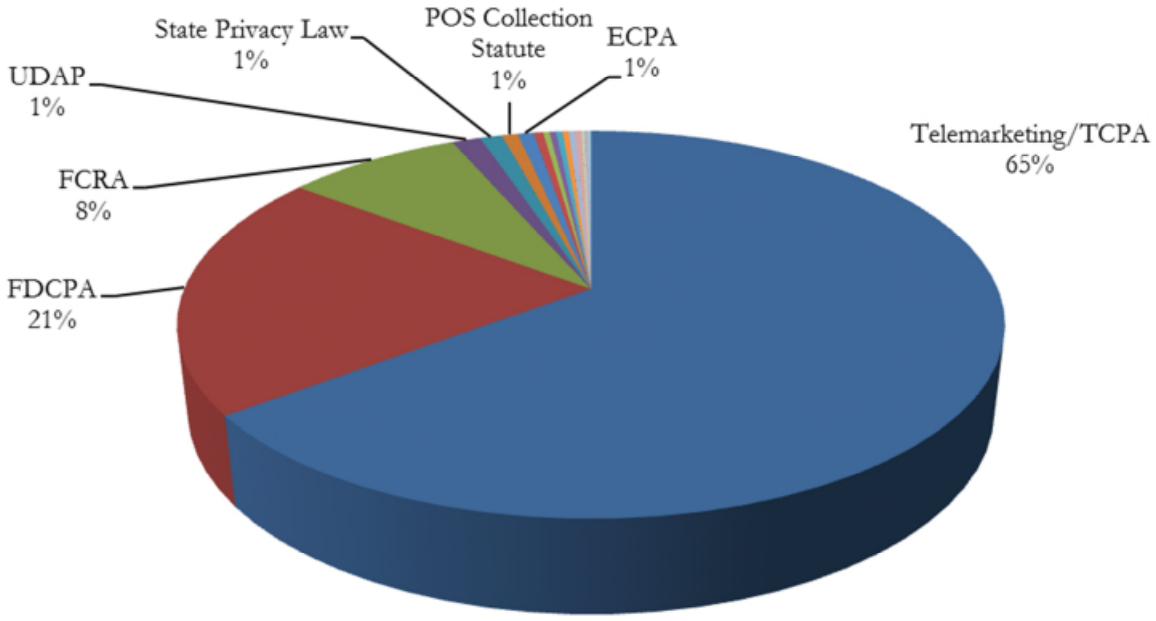
## Part 5: Primary Legal Theories

Our prior data privacy Reports have shown a historical bias by the plaintiff's bar to bring data privacy litigation relating to the use of telemarketing based upon alleged violations of the Telephone Consumer Protection Act ("TCPA"). The TCPA continues to dominate the landscape of data privacy litigation with 436 class action complaints filed during the Period – constituting 65% of all data privacy related class actions.

In total, there were 19 different primary legal theories alleged.[7] As discussed in Part 3, debt collectors as an industry received the most class action complaints; perhaps not surprisingly, therefore, the second most popular primary legal theory alleged was a privacy violation under the Fair Debt Collection Practices Act ("FDCPA") (21%).

Interestingly the defense bar does not appear to be focused on the same privacy statutes as the plaintiff's bar. For example, while defense firms have written 4 times the quantity of bulletins, alerts, and articles about California's Song Beverly Credit Card Act (a point of sale collection statute) than the FDCPA, there were 21 times more privacy litigation cases premised on the FDCPA than on Song Beverly.[8]

The following chart provides a detailed breakdown of the primary legal theories alleged during the Period:



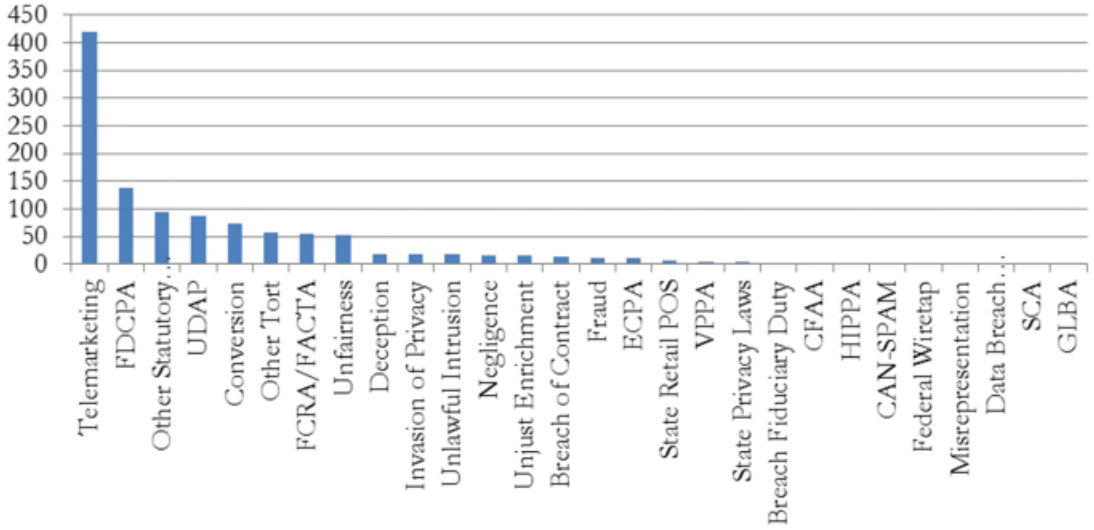

7 While not identified in the chart, the following primary legal theories each constituted less than 1% of all claims filed: VPPA; TCPA/FDCPA; Deception; Unfairness; Fraud; Other Statutory Violations; Invasion of Privacy; CAN-SPAM; Breach of Contract; and HIPAA.

8 These estimates were obtained via a Lexology search of "Song Beverly," which returned 1,766 results and "FDCPA," which returned 430 results. The search was conducted on May 10, 2015.

## Part 6: Variety of Legal Theories Alleged

Our analysis of the data privacy complaints identified not only the primary legal theory alleged, but any secondary or alternative theories alleged in the complaints. As reflected in the chart below, although plaintiff's attorneys showed a clear preference for bringing suit based upon telemarketing and the TCPA, the plaintiff's bar pursued 28 different privacy theories.

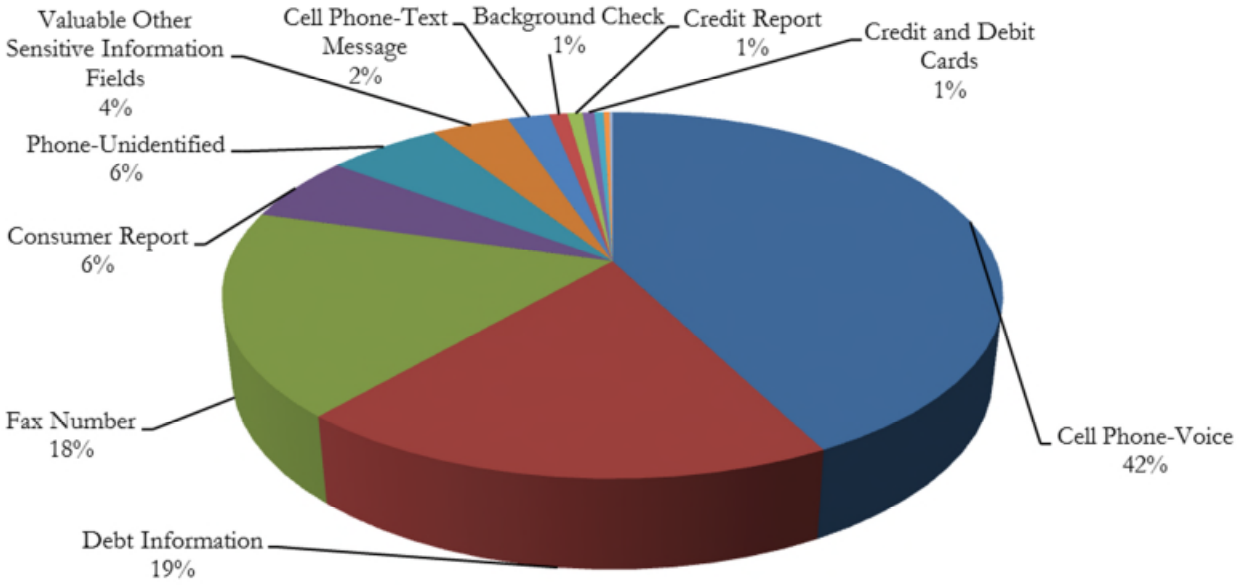
The following chart provides a detailed breakdown of all of the theories utilized by plaintiff's attorneys in privacy litigation cases during the Period:



## Part 7: Primary Type of Information at Issue

Consumers today are more concerned about the privacy of their information than ever. 91% of adults in a 2014 Pew Research survey agreeing or strongly agreeing that "consumers have lost control over how personal information is collected and used by companies."[9] 38% of adults in a 2015 TRUSTe survey identified companies' collection and sharing of personal data as one of their top concerns.[10] Little research has been conducted, however, concerning the type of data that consumers most fear will be misused.

As indicated in Part 6, litigation cases focus overwhelmingly on the privacy of telephone numbers. Collectively telephone numbers – whether used to call a cell phone, landline, fax machine or to send a SMS text – accounted for 68% of all litigation. Note that while our data breaks down how telephone numbers were allegedly used (*e.g.*, voice, text, etc.) the quantity of text messaging cases may be under reported as many plaintiff's attorneys did not specify whether a cell phone number was used to send voice, text, or both.




9 *See* Public Perceptions of Privacy and Security in the Post-Snowden Era *available at* http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/ (last visited April 21, 2015).

10 *See* TRUSTe Privacy Index: 2015 Consumer Confidence Edition *available at* http://www.slideshare.net/trusteprivacyseals/2015-truste-us-consumer-privacy-confidence-index-infographic (last viewed April 21, 2015).

## Part 8: Plaintiffs' Firms

Over 240 plaintiffs' firms filed class action complaints related to data privacy. While 70% of plaintiffs' firms (*i.e.*, 169 firms) filed only one complaint during the Period, there were four plaintiffs' firms that filed a disparate number of complaints (73, 70, 51, and 41 respectively). As a result, roughly 1.5% of the plaintiffs' firms involved in data privacy litigation accounted for over one third of the complaints filed.

## 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:

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

- "collect" or "share" or their derivations and "zip," "address," "email," or "number," at a reasonable distance in the text from "personal," "customer," or "consumer."

Additional searches were used to identify complaints that specifically referenced the Telephone Consumer Protection Act ("TCPA"), the Controlling the Assault of Non-Solicited Pornography and Marketing Act ("CAN-SPAM"), 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"), the Electronic Communications Privacy Act ("ECPA"), and point-of-sale ("POS") statutes, including the California Song Beverly Credit Card Act.

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 based upon the availability of access to state complaints. Complaints which are removed from state court to federal court were included within the analysis.

## AUTHORS

**David Zetoony** is the leader of Bryan Cave's 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 the firm'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

**Leila Knox** focuses her practice on 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.

**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 400 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.