Data Breach Litigation Report

2019 Edition

Jena Valdetero
Partner, Chair Data Security Practice

David Zetoony
Partner, Chair Data Security Practice

Andrea Maciejewski
Data Privacy and Security Team Member

BRYAN CAVE LEIGHTON PAISNER BCLP

bclplaw.com

Executive Summary

Both 2017 and 2018 saw several high-profile companies suffering large data breaches affecting tens of millions of people. News outlets and social media made quick work of headlines and consumers were reminded, yet again, that their personal information was vulnerable and subject to theft. The now-tired adage, "it's not a matter of *if*, but *when* you will be breached" was trotted out by experts and the media alike, making it sound as if a data breach inevitably leads to a class action lawsuit against the targeted company.

But the untold story was the 600+ publicly reported data breaches per year that *did not* make the news and that *did not* result in class action litigation. Despite numerous large and public data breaches, the risk that a company will face litigation following a data breach remains relatively low year-after-year, between 4-6%, consistent with prior years' studies published by our firm.

Despite the numbers, news outlets and players in the cybersecurity space can be powerful purveyors of misinformation, and we continue to see organizations misunderstand their risks of litigation after a data breach. Our goal is to help companies accurately evaluate the costs and risks flowing from a data breach and allocate resources in proportion to the risk of harm.

Bryan Cave Leighton Paisner began its survey of data breach class action litigation six 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 2019 report covers federal class actions initiated between January 1, 2017 and December 31, 2018. The data is split into two periods that cover January 1, 2017 to December 31, 2017 and January 1, 2018 to December 31, 2018. Our key findings are:

- Increase in filings since 2016.
    - 2017: 152 class actions were filed during 2017. This represents a **100% increase in the quantity of cases filed as compared to the 2017 Data Breach Litigation Report** ("2016").[1]
    - 2018: 103 class actions were filed during 2018. This represents a **48% decrease in the quantity of cases filed as compared to 2017, but a 26% increase for 2016.**
- Continued "lightning rod" effect. The majority of the complaints cluster around 2-4 high-profile breaches. When multiple filings against a single defendant are removed,

[1] There were 76 complaints filed in 2016. *See* Bryan Cave Leighton Paisner, 2017 Data Breach Litigation Report.

there were 26 unique defendants in 2017 and 36 unique defendants in 2018. 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 reporting data breaches.

- Increase in filings as a function of the quantity of breaches.

    - 2017: **Approximately 4.0% of data breaches publicly reported in 2017 led to class action litigation.** This is a slight increase from 2016, in which only 3.3% of publicly reported data breaches led to class action litigation relative to the number of breaches.

    - 2018: **5.7% of data breaches publicly reported in 2018 led to class action litigation in 2018.** This is a 1.7% increase from 2017 and a 2.4% increase from 2016, indicating a steady increase in class action litigation relative to the number of breaches.

- California is a preferred litigation forum regardless of the location of defendant. Unlike previous years, the choice of forum, while occasionally motivated by the states in which the defendant companies are based, **were more likely to be in either the Northern District of California or the Central District of California.** These two districts accounted for 28% of all class action data breach litigation during 2017 and 39% of all class action data breach litigation during 2018.

- Medical record breach litigation declined. **The percentage of class actions involving the breach of medical records fell from 2016,** with medical information accounting for 3% of litigation in 2017 and 1% in 2018. This may reflect a lack of high profile medical record breaches or an increase in attention to data breaches involving other types of records.

- Plaintiffs continue to use an increasing number of legal theories. Plaintiffs' attorneys continue to allege multiple legal theories. **Plaintiffs alleged a total of 24 legal theories during 2017 and 26 legal theories during 2018**.

- Negligence is still a clear theory of preference. Negligence, the most popular legal theory in 2016, **remained the primary theory (first legal count) in approximately 50% of all class action complaints and was alleged in over 90% of all class action complaints during both 2017 and 2018.**

Forecast: Based on the consistency of data over the last six years, we anticipate that 2019 will produce similarly low numbers of class action lawsuits filed compared to the overall number of reported breaches. However, we do not expect this trend to continue following the effective date of the California Consumer Privacy Act ("CCPA") in January 2020. The CCPA is on target to be the first state law to provide statutory damages to individuals affected by a data breach. California residents whose information is breached will have the ability to bring suit against

companies that are subject to CCPA compliance. With its express reference to "class actions," and the ability to recover attorney's fees for successful plaintiffs, it seems inevitable that we will see a significant uptick in data breach class actions filed in California courts.

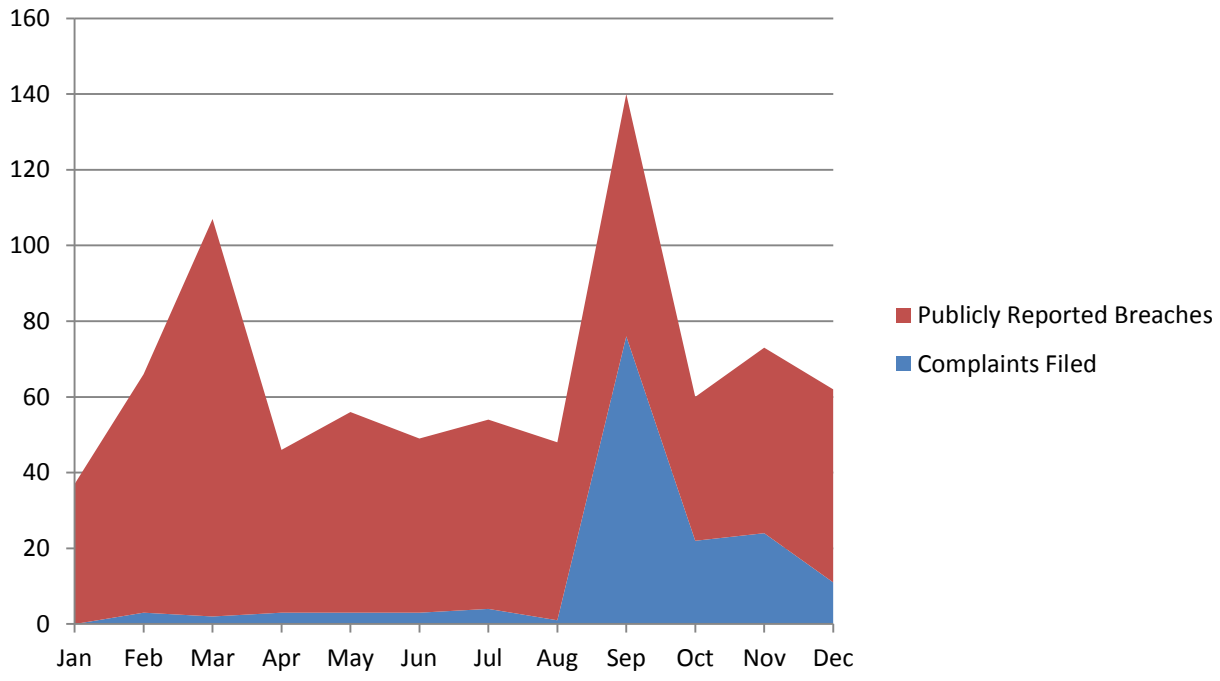
Part 1: Volume of Litigation

2017:

A total of 152 complaints were filed during 2017, up 100% from 2016. According to the Privacy Rights Clearinghouse Chronology of Data Breaches ("Privacy Rights Clearinghouse"), 646 breaches were publicly reported during 2017, down 20% from publicly reported breaches in 2016. Out of the 152 federal class action complaints arising from a data breach filed during 2017, there were only 26 unique defendants. As a result, approximately 4.0% of publicly reported breaches led to class action litigation. The overall result is that there was not a significant increase in the rate of complaint filings between 2016 and 2017 when total complaints are normalized by unique defendants and the quantity of breaches.

There was no month-to-month correlation between the number of publicly reported breaches and the number of class action complaints regarding data breaches. For example, in March of 2017 there was a 67% increase in publicly reported breaches whereas there was a 33% decrease in complaints filed. Conversely, in September of 2017, the Equifax data breach caused a 7500% uptick in complaints filed whereas publicly reported breaches only increased by 36%.

The following charts provide a breakdown of class action complaints filed with the quantity of publicly reported breaches disclosed during 2017.



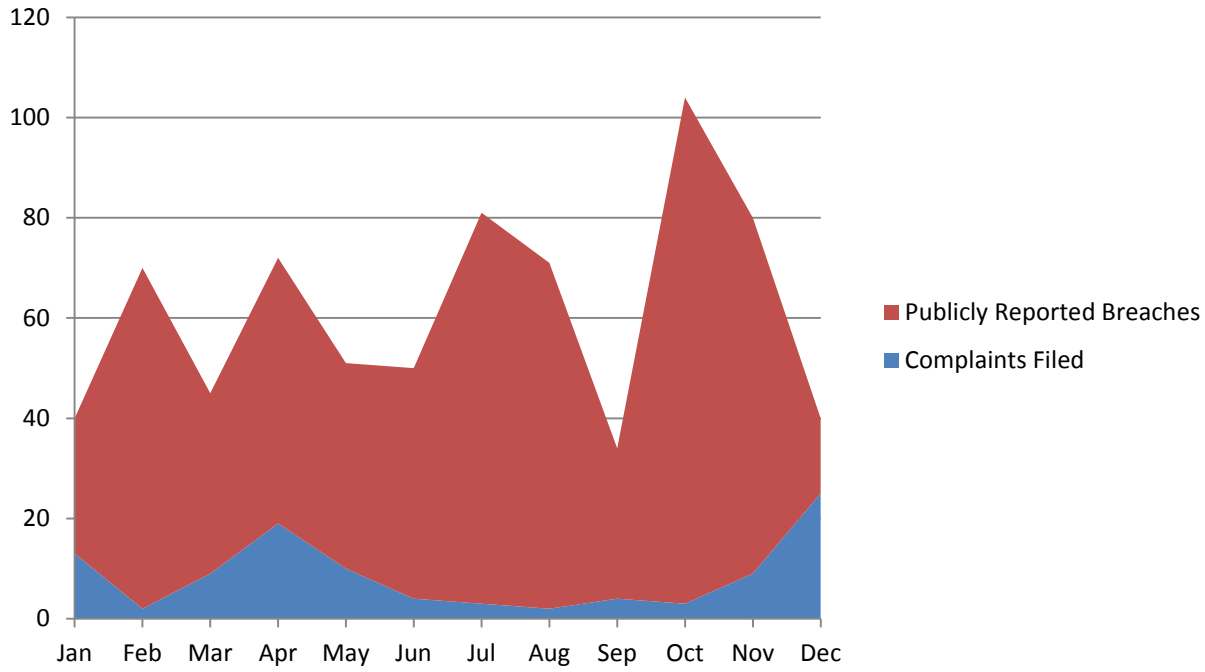
2018:

A total of 103 complaints were filed during 2018, down 48% from 2017, but up 26% from 2016. According to the Privacy Rights Clearinghouse, there were 635 publicly reported data breaches

in 2018. Out of the 103 federally filed class action complaints, there were 36 unique defendants. As a result, 5.7% of publicly reported data breaches led to class action litigation. This indicates a slight increase in the rate of complaint filings from 2017.

Similar to 2017, the quantity of litigation does not correlate with the number of publicly reported breaches each month. Other than increases in complaints against Facebook and Marriot in February and December respectively, the number of complaints was relatively steady from month to month.

The following charts provide a breakdown of class action complaints filed with the quantity of publicly reported breaches disclosed during 2018.



Part 2: Favored Courts[2]

In previous years, the preferred forums for filing data breach class action litigation tended to correlate with the location of the defendant company's headquarters. In both 2017 and 2018, this trend declined, and we saw a general increase in litigation filed in California courts. This may be due to the California Supreme Court's 2017 decision in *McGill v. Citibank*, which held that arbitration provisions foreclosing an individual's right to seek statutory remedies are

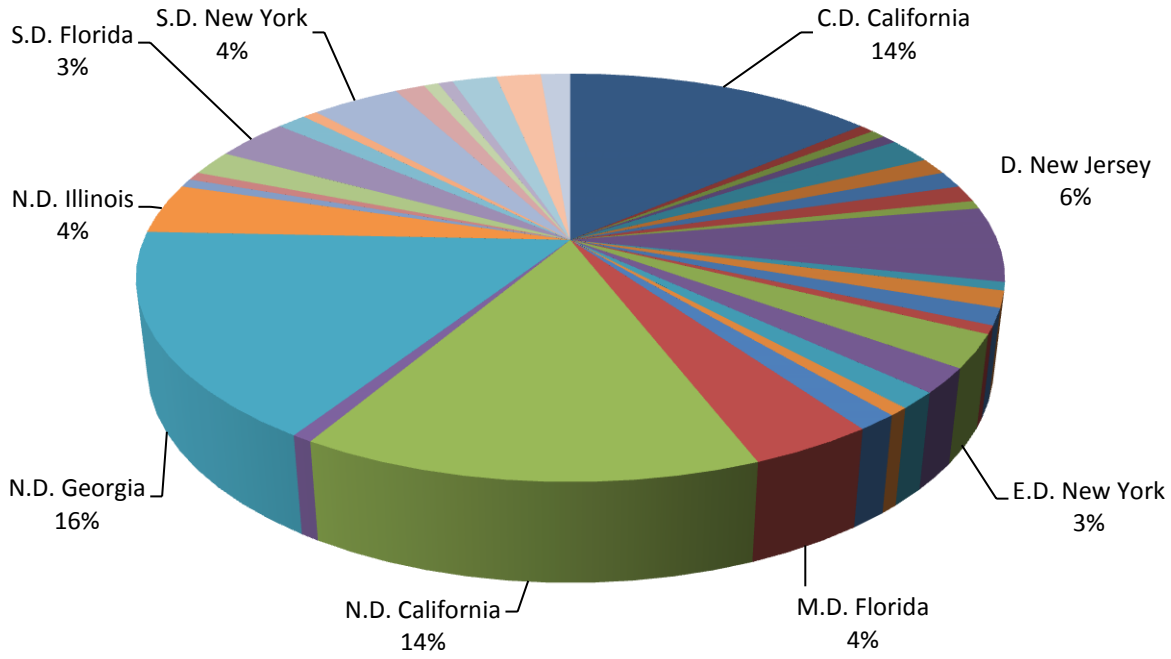
[2] This report does not include complaints filed in state courts. For more information, please see Part 9: Methodology.

unenforceable.[3] This makes it possible for plaintiffs nationwide to try and circumvent class action waivers in arbitration agreements by filing their class action lawsuits in California.

2017:

There were three preferred forums for filing data breach class action litigation in 2017: the Northern District of Georgia, the Northern District of California, and the Central District of California. These three courts combined to account for approximately 45% of all filings. Although the concentration of litigation was somewhat related to the location of the defendant company's headquarters, the correlation was not as strong as in recent years. For example, the 107 complaints filed against Equifax, 23 were filed in the Northern District of Georgia (Equifax's headquarters), 15 were filed in the Northern District of California, and 11 were filed in the Central District of California. The remaining 58 complaints were scattered among 27 other forums. Similarly, only 50% of the complaints filed against Sonic were filed in the Western District of Oklahoma (the location of Sonic's headquarters).

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



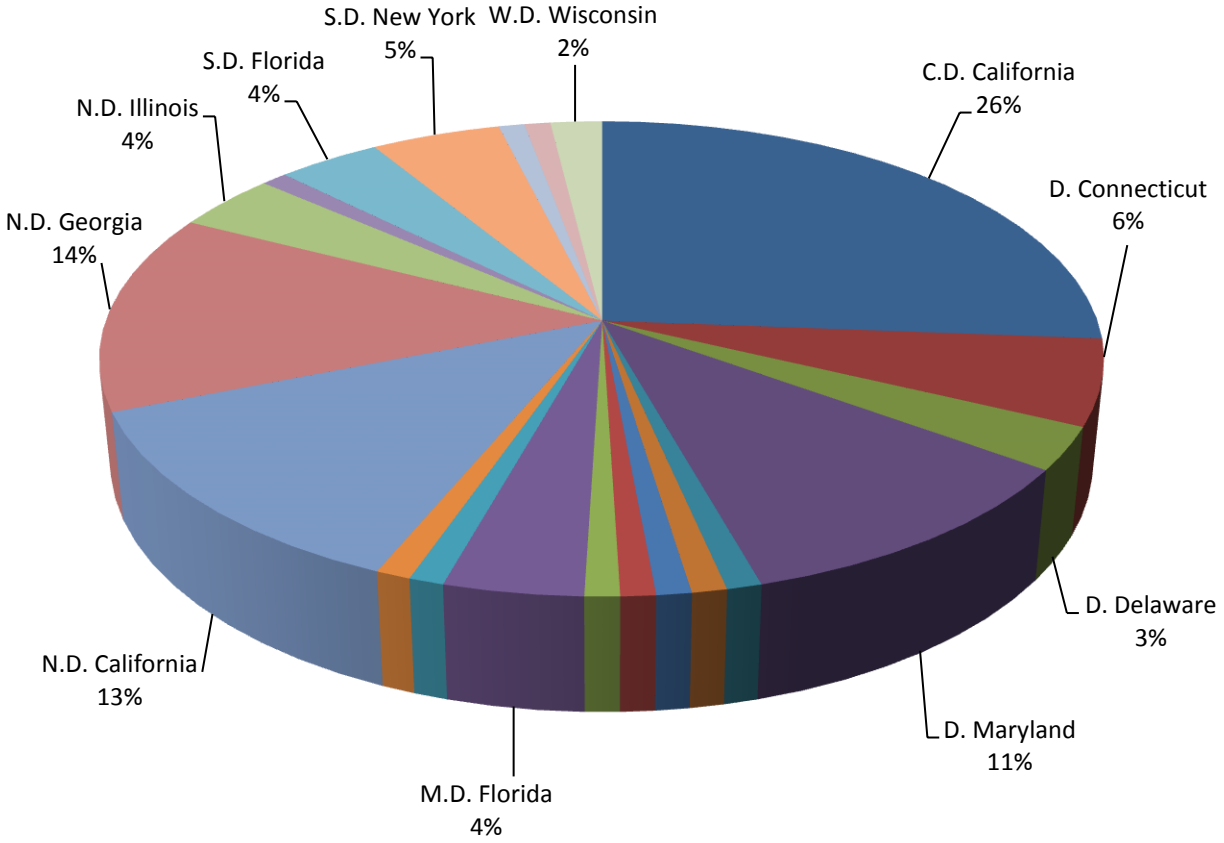
[3] 2 Cal.5th 945, 959-61 (2017).

[4] The following courts are not labeled in the chart and each represent between 1%-2% of the total filings during the Period: District of Arizona, District of Colorado, District of Connecticut, District of Delaware, District of the District of Columbia, District of Maryland, District of Nevada, District of New Hampshire, District of Rhode Island, District of South Carolina, District of Vermont, Eastern District of California, Easter District of Pennsylvania, Eastern District of Texas, Eastern District of Virginia, Eastern District of Wisconsin, Northern District of New York, Northern District of Ohio, Northern District of Texas, Southern District of Indiana, Southern District of Mississippi, Southern District of Texas, Southern District of West Virginia, Western District of Kentucky, Western District of North Carolina, Western District of Oklahoma, and Western District of Washington.

2018:

The Central District of California was the preferred forum for filing class action data breach litigation in 2018, with approximately 26% of all filings originating in that court. Once again, there was a slight correlation between the location of litigation and the location of the defendant company's headquarters, but it does not appear to be the primary driver of preferred forum. For example, of the 27 complaints filed in the Central District of California, only 2 were against companies headquartered in that district. However, an increase in filings in the District of Maryland was directly attributable to a data breach involving Marriott International (which is headquartered in Maryland).

The following provides a detailed breakdown by district of federal class action filings:[5]



[5] The following courts are not labeled in the chart and each represents 1% of the total filings during the Period: District of Minnesota, District of Nevada, District of New Mexica, District of Utah, Eastern District of Pennsylvania, Middle District of Tennessee, Northern District of Alabama, Northern District of Ohio, Southern District of Texas, and Western District of Texas.

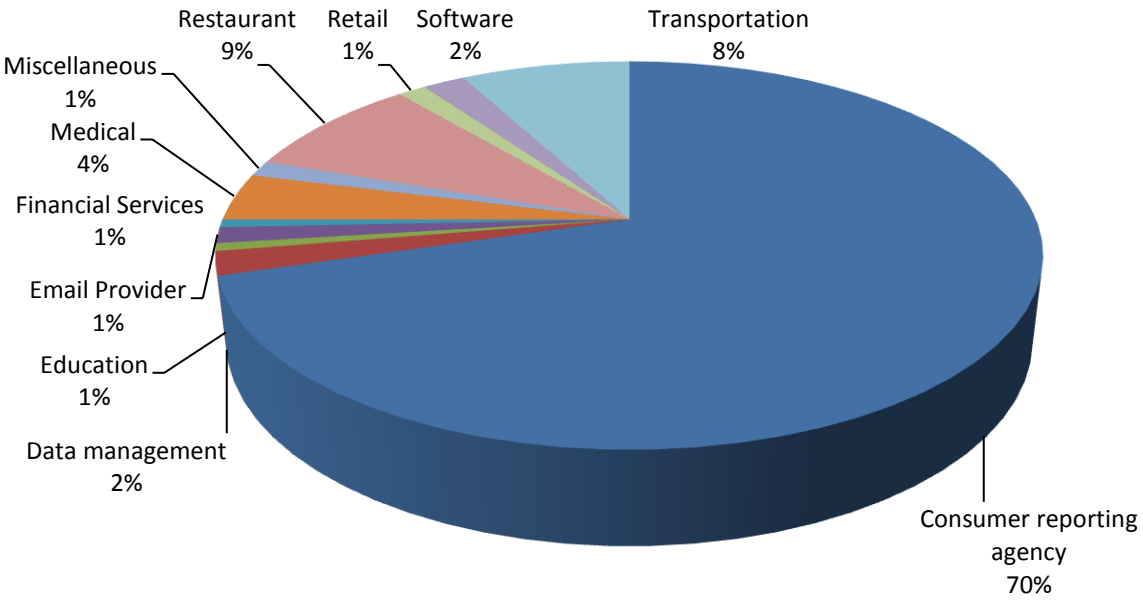
Part 3: Litigation by Industry

2017:

The consumer reporting agency industry was the target of the majority of class action complaints in 2017 (70%), with 107 complaints filed against it. The restaurant industry and the transportation industry were also major targets of class action data breach complaints, accounting for 9% and 8% of all complaints in 2017 respectively.

2017 saw an explosion of class actions against Equifax related to the announcement of a security breach involving, among other things, the social security numbers and financial information of over 140 million people. Experiencing a slight decrease from 2016, the restaurant industry remained the target of class action complaints due to a new security breach affecting many restaurant's point of sale technology, with class actions filed against companies such as Sonic, Arby's, and Chipotle. Finally, the transportation industry emerged as a target of class action complaints following the discovery of a 2016 data breach at Uber. In contrast, the email provider industry and the medical industry both saw steep declines in class actions. While the email provider industry had few to no publicly reported data breaches, the medical industry was not so lucky. Consistent with trends from previous years, more than 66% of publically reported breaches in 2017 involved the medical industry. The contrasting decline in class actions could be attributable to larger, more public breaches that overshadowed medical industry breaches. It could also be that many of the publically reported breaches in the medical industry were from smaller entities that likely presented lower recovery potential for plaintiffs' attorneys than major corporate breaches at well-known companies.

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

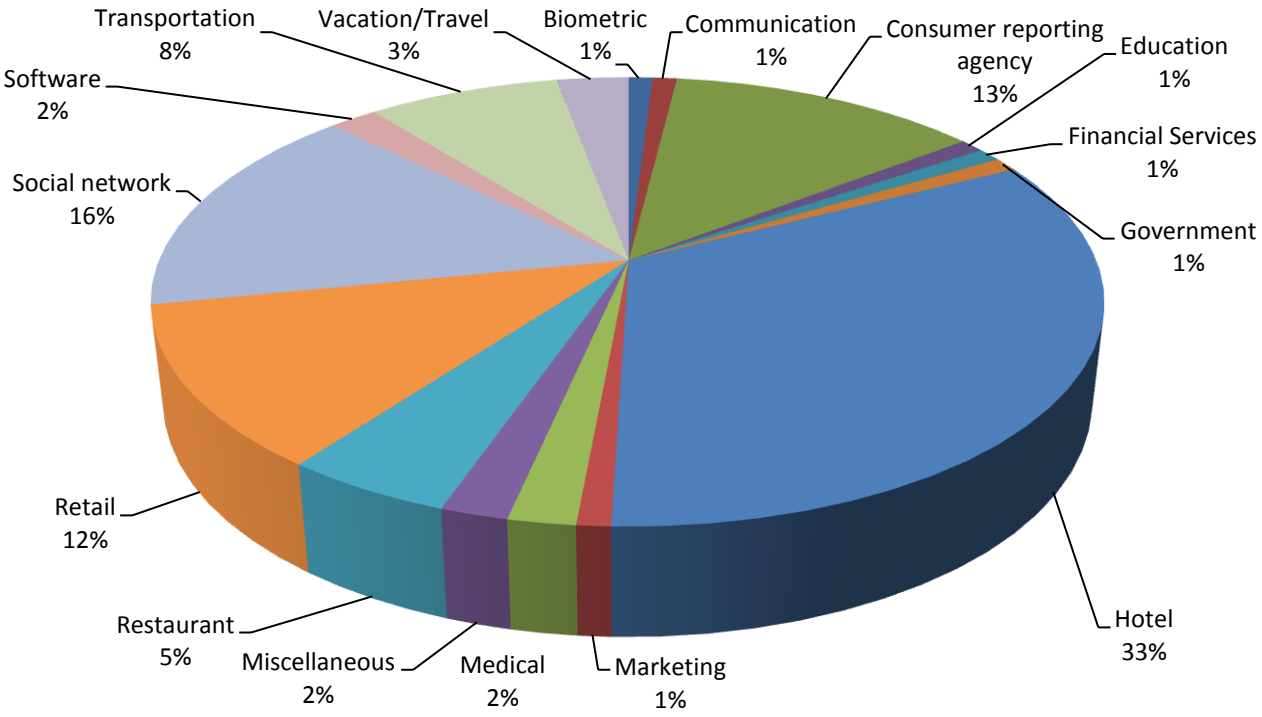


2018:

The hotel industry was the target of the majority of class action complaints in 2018 (33%), with 34 complaints filed. The social network industry was the target of 16% of complaints, with 16 complaints filed. Neither industry was the target of any complaints during 2017.

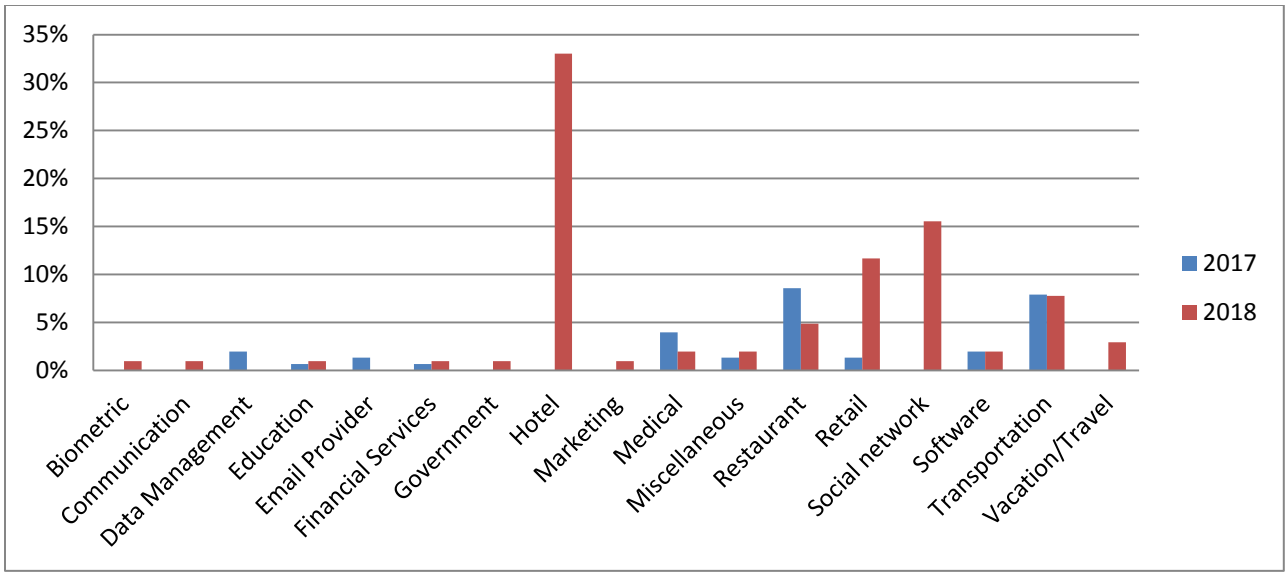
Marriott International saw numerous class actions due to a breach of its reservation system that affected over 500 million people. There were also multiple class actions against Facebook following Cambridge Analytica's alleged unauthorized mining and misuse of over 87 million Facebook user's personal and profile data. Litigation against Equifax slowed down significantly, but still saw 13 complaints filed in 2018.

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



When controlling for the consumer reporting industry, the following chart provides a comparative view of defendant industry between 2017 and 2018:[6]

[6] The Consumer Reporting Industry accounted for 70% of litigation in 2017 and 13% of litigation in 2018.



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. For this reason, 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.

In both 2017 and 2018, there was a strong preference for class actions that were national in scope. This is consistent with previous years and may mean that plaintiffs' attorneys prefer to allege putative national classes in an attempt to obtain potentially greater recovery. It also could reflect the fact that most, if not all, of the companies who had class action data breach complaints filed against them in federal courts 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 and were not removed by the defendant to federal court.

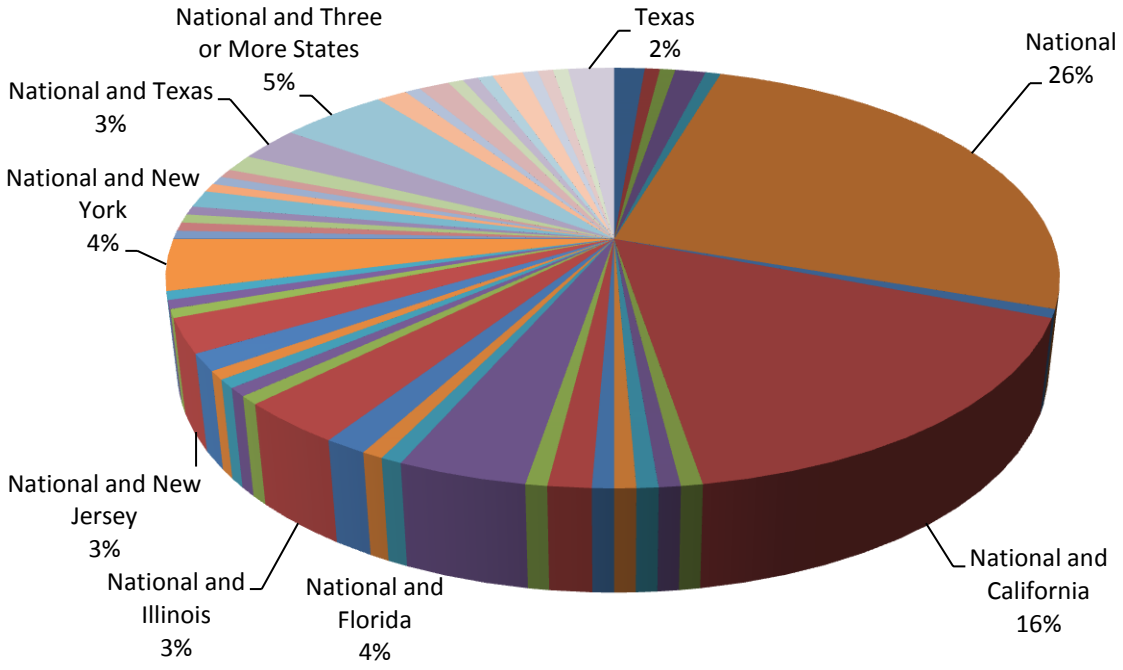
Despite the consistent preference for national classes in both 2017 and 2018, we see some notable differences between the two years.

2017:

In 2017, 89% of complaints alleged a national class or a national subclass. In fact, 26% of all class action complaints only alleged a national class (with no state-specific sub-class). The other 74% of complaints alleged a sub-class tied to residents in specific states, which is a 25% increase

from 2016. The most common state sub-class was California, with complaints alleging a national class and a California sub-class accounting for 16% of all complaints.

The following chart provides a breakdown of the scope of putative classes:[7]



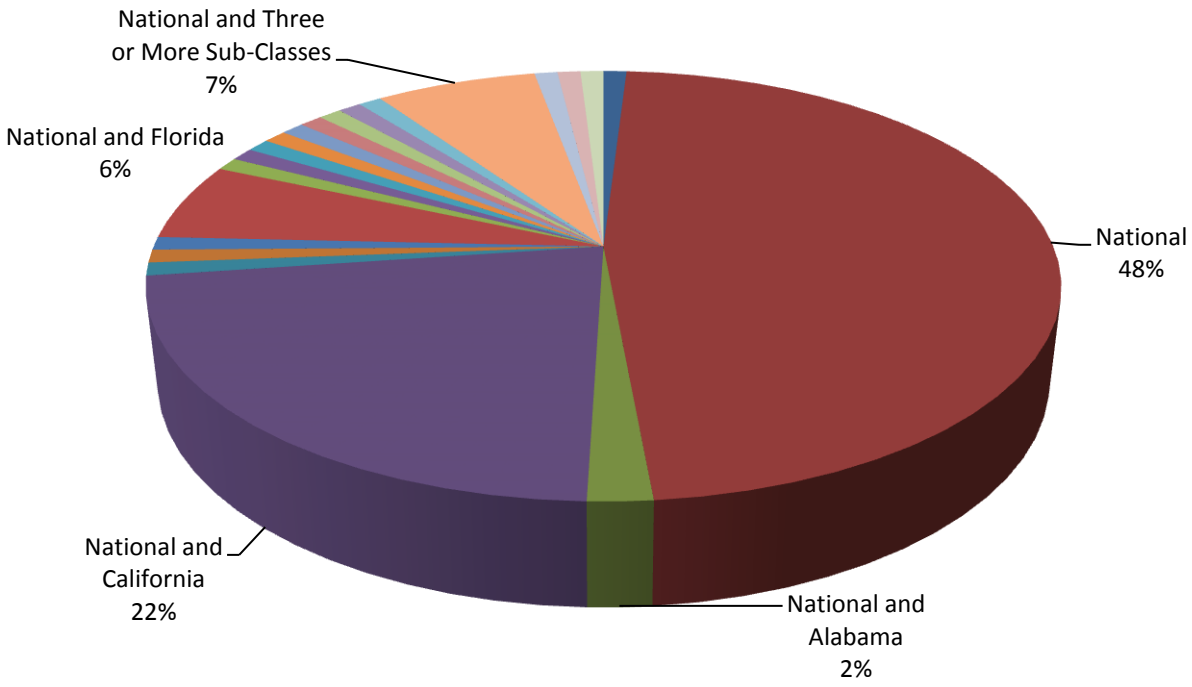
2018:

The number of complaints that alleged a national class or a national subclass increased to 98% in 2018. Correspondingly, the number of class action complaints that alleged a national class with no sub-class also increased to 48%. The most common state sub-class was once again California, with complaints alleging a National class and California sub-class accounting for 22% of all complaints.

The following chart provides a breakdown of the scope of putative classes: [8]

[7] Only putative classes that accounted for over 1% are shown. There are 43 other putative class combinations, which are not noted in this survey.

[8] 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: California, National and California and Florida, National and California and Illinois, National and Colorado, National and Florida and New York, National and Maryland, National and Maryland and California, National and Massachusetts, National and Missouri, National and Nevada, National and New Jersey and Pennsylvania, National and New York, National and Texas, National and Utah, National and Washington, Ohio.

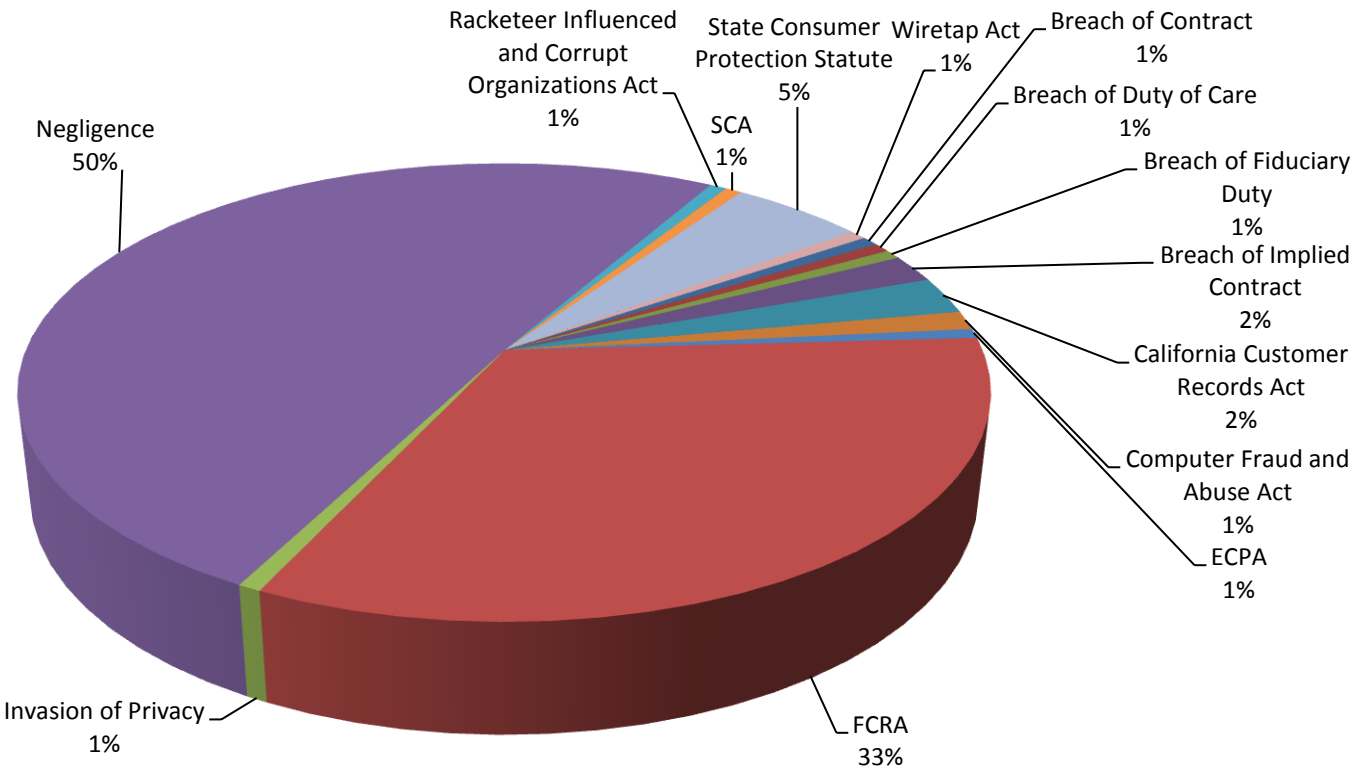


Part 5: Primary Legal Theories

2017:

In 2017, Plaintiffs continued to pursue negligence as the predominant theory under which they sought recovery (*i.e.*, the first count alleged in a complaint), although its popularity declined slightly with 51% of all class action litigation alleging negligence as the primary theory (compared to 65% in 2016). The decrease could be attributed to the number of complaints against Equifax and the related increase in the FCRA's use as a primary theory (33%). Complaints alleging state consumer protection statutes as a predominant theory declined from 16% in 2016 to 5%. Overall, there was a wider variety of theories used as a primary claim, with Plaintiffs alleging 14 different theories, an increase from 6 different theories used in 2016.

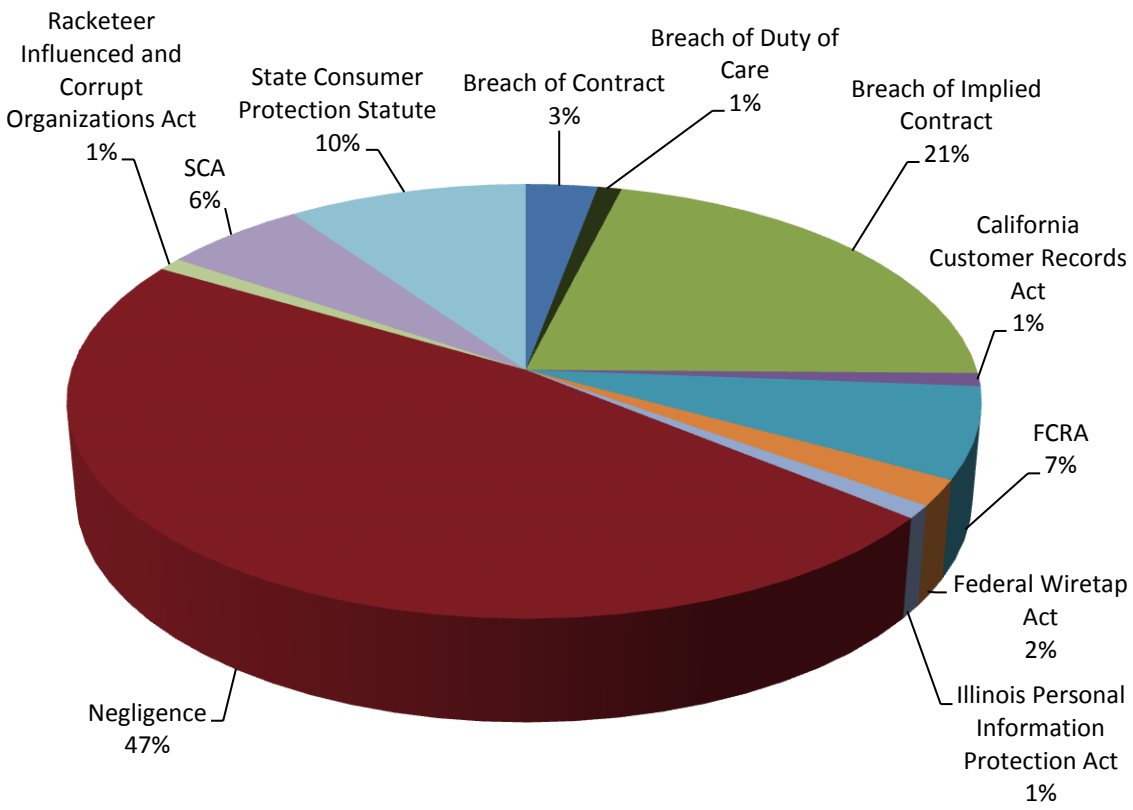
The following provides a breakdown of the primary theory alleged:



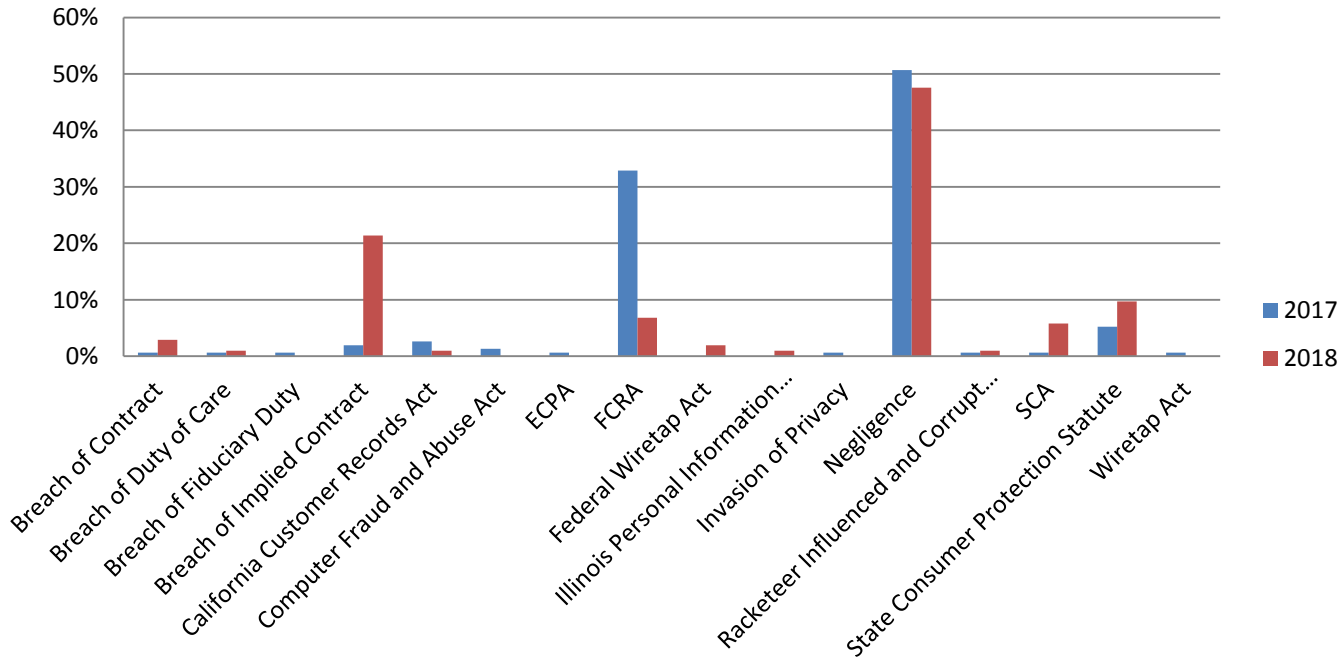
2018:

Negligence continued to be the predominant primary theory during 2018 (47%). Allegations of breach of implied contract emerged as a trend in 2018, with 21% of complaints using this as the primary theory. These claims were typically used against retail stores whose point of sale system was breached. In contrast, there was a sharp decline in the use of the FCRA as a primary theory, correlating with the decrease in complaints against Equifax. The variety of theories alleged dropped to 11 which, although lower than 2017, is still almost double the number of theories alleged in 2016.

The following provides a breakdown of the primary theories alleged:



The following chart provides a comparative view of primary theories alleged in 2017 and 2018:



Part 6: Variety of Legal Theories Alleged

In both 2017 and 2018 almost all plaintiffs chose to allege more than one theory of recovery, with plaintiffs' attorneys alleging an average of 4 to 5 theories per complaint. Many complaints combined theories sounding in contract, tort, and statute.

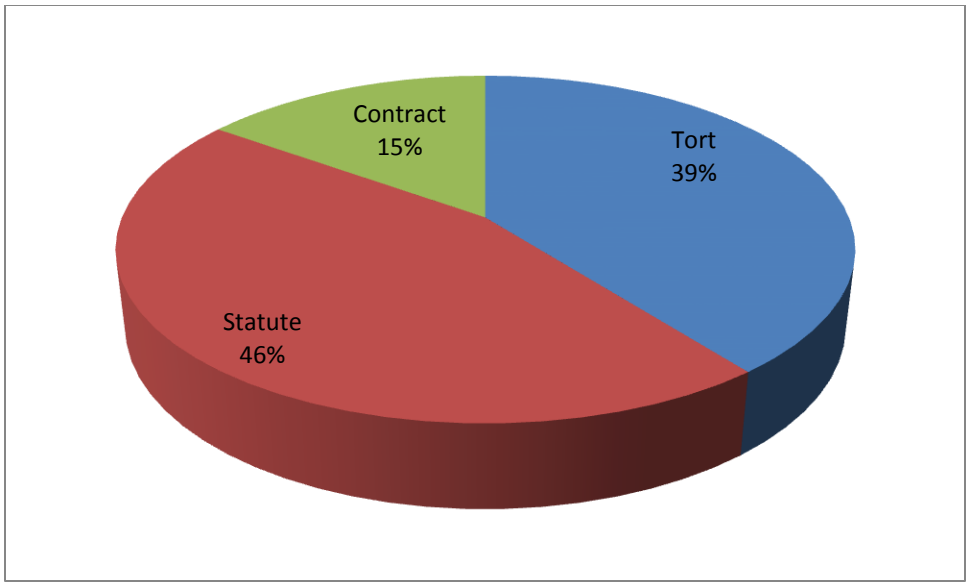
Two new data points that we chose to track for both years was (1) the allegation of a failure to detect a data breach and (2) the allegation of a failure to notify data subjects of a data breach (either in a timely manner or at all). The failure to notify was alleged in 88% of 2017 complaints and 86% of 2018 complaints. When controlling for defendants with multiple claims against them, the percentage falls to 50% and 41% respectively. Every defendant that was the target of the lightning rod effect, with the exception of Sonic, had all or the vast majority of the complaints against it allege a failure to notify. Only 6% of complaints over the course of 2017 and 2018 alleged *neither* a failure to notify *nor* a failure to detect. With the exception of Sonic, **none** of these complaints were against a defendant who was the target of the lightning rod effect.

These numbers indicate a relationship between the failure to notify and the likelihood of being a target of the lightning rod effect. Further, the lack of complaints alleging at least one failure could mean that an organization's detection of and response to a data breach reduces the likelihood of class action litigation.

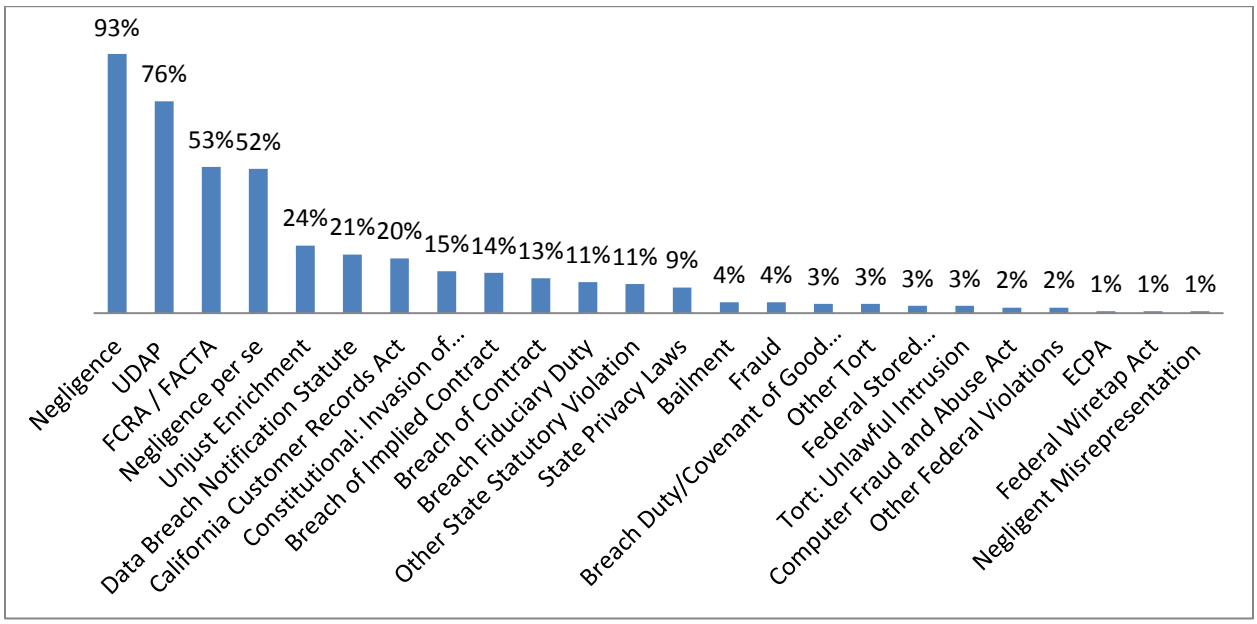
2017:

In 2017, plaintiffs pursued a total of 24 different legal theories of recovery, showing a preference for negligence, state consumer protection statutes, and the FCRA. In addition to being the most common primary theory used, negligence was alleged in 93% of cases. State consumer protection statutes were alleged 53% of the time and continued to see an increase in use from 2016. The claim of negligence per se emerged as a new trend and was used primarily to invoke Section 5 of the Federal Trade Commission Act for the failure to implement reasonable security measures to protect sensitive information.[9] Most contract-based claims (e.g. breach of contract, breach of fiduciary duty, etc.) fell from previous years, potentially because many of the major breaches did not have an express contract between the data subject and the organization that experienced the data breach. This relationship between the data subject and the defendant organization also led to the use of breach of implied contract as a legal theory, the only contract-based claim that increased from 2016. A breakdown of theories based in contract, tort, and statute is below:

[9] Section 5(a) of the Federal Trade Commission Act makes unfairness and deception towards consumers unlawful. 15 U.S.C.A. § 45.



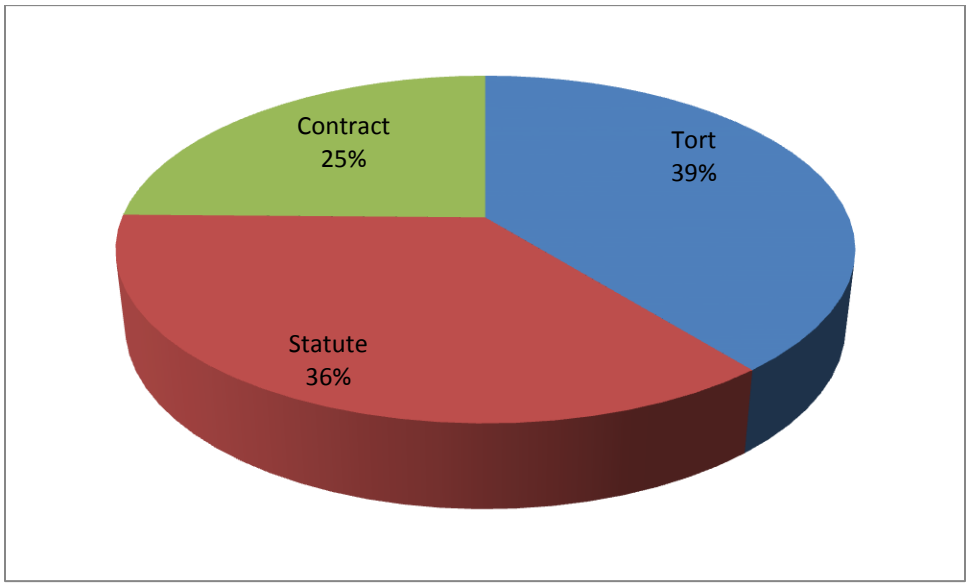
The following chart provides a detailed breakdown of the theories utilized by plaintiffs' attorneys in data breach litigation complaints during 2017:



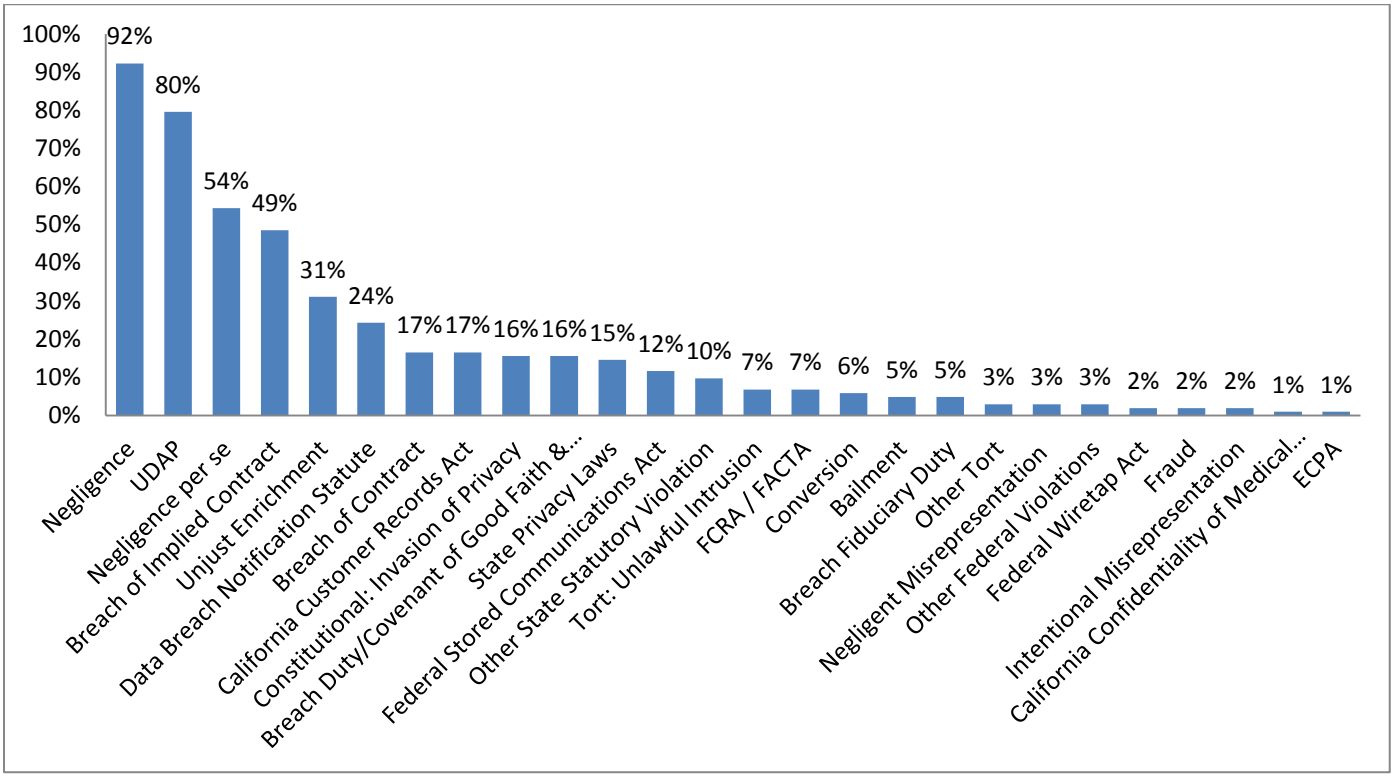
2018:

Many of the trends from 2017 continued into 2018. Negligence (92%), state consumer protection statutes (80%), and negligence per se (54%) were again highly utilized by plaintiffs. Claims for breach of implied contract were included in almost 50% of all complaints (up from 14% in 2017). Overall, the variety of theories used rose to 26. There was a sharp decline in the

use of FCRA due to the abatement of claims against Equifax. A breakdown of theories based in contract, tort, and statute is below:



The following chart provides a detailed breakdown of the theories utilized by plaintiffs' attorneys in data breach litigation complaints during 2017:



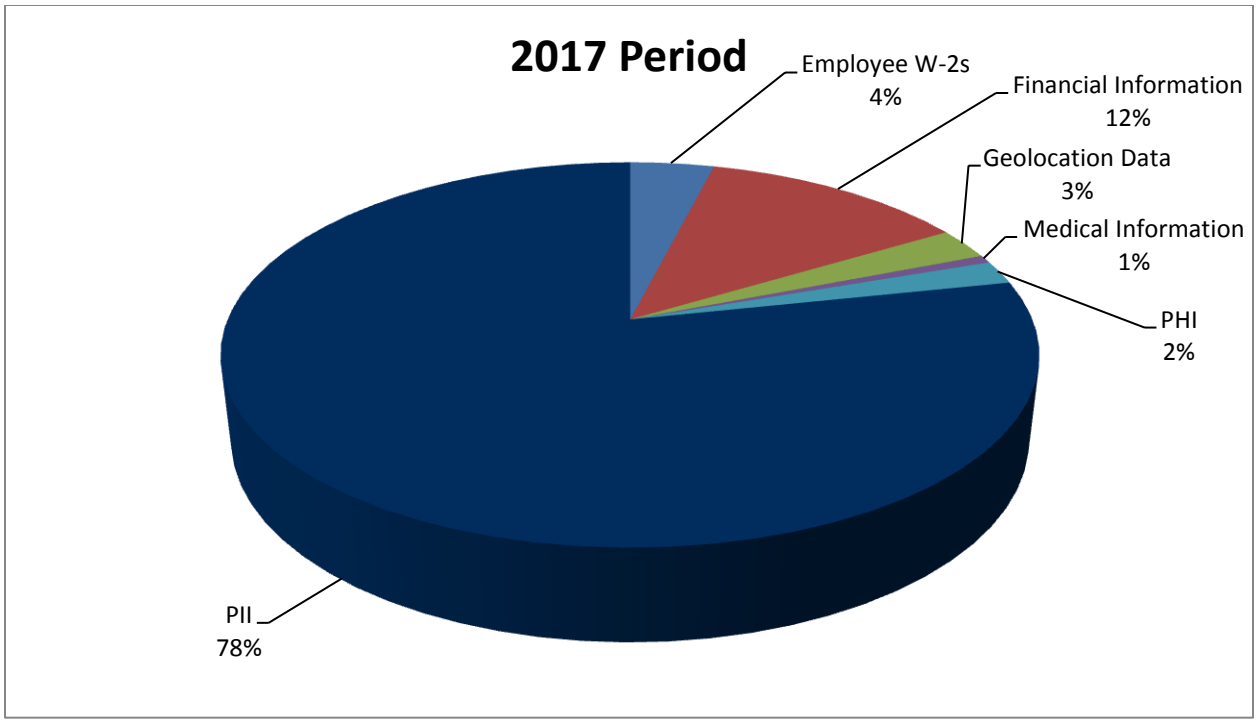
Part 7: Primary Type of Data at Issue

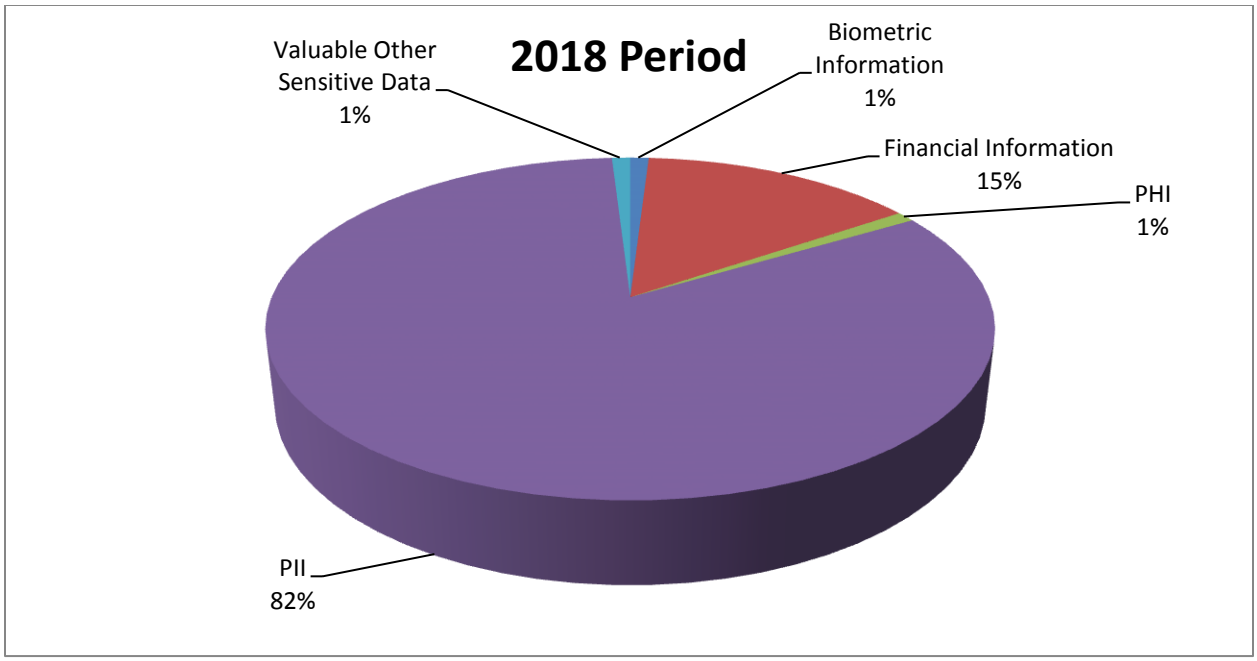
Historically, data drawn from medical records was the largest focus of publically reported breaches and class action lawsuits. However, 2017 and 2018 both saw a sharp decrease in the number of class action complaints regarding data breaches that were focused on medical information. Only 3% of class actions in 2017 and 1% of class actions in 2018 targeted companies who experienced a breach of health information, down from 34% of class actions in 2016.

In contrast, driver's license numbers and social security numbers (collectively, "PII") were the focus of 72% of complaints during 2017 and 82% of complaints during 2018. 68% of complaints during 2017 also focused on credit cards and debit cards (collectively, "financial information") as a secondary type of data at issue, correlating to the amount of litigation against Equifax. This secondary focus on financial information fell to 22% in 2018.

Given the type of industries that were the target of the largest breaches in 2017 and 2018, it is no surprise that the primary types of data at issue were PII and financial information. Despite the relative value of individual medical records, breaches that lead to the disclosure of tens of millions of credit card numbers hold immense value in the aggregate. As such, cyber security theft targeting large organizations may have increased because they are more lucrative than thefts targeting smaller organizations.

The following chart provides a detailed breakdown of the type of data involved in data breach litigation for 2017 and 2018:





Part 8: Plaintiffs' Firms

In 2017, more than 113 plaintiffs' firms participated in filing class action complaints related to data security breaches. Although most plaintiffs' firms filed between 1 and 3 complaints, one firm filed six class action lawsuits.

2018 saw a similar trend, although fewer firms participated overall. There were a total of 72 plaintiffs' firms that filed class action complaints related to data security breaches. However, it was slightly more common for a plaintiffs' firm to file more than one complaint, with multiple firms filing 4 or more complaints during the Period.

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, and Bloomberg Law databases. 2017 covered January 1, 2017-December 31, 2017. 2018 covered January 1, 2018-December 31, 2018. Multiple searches were run in order to find complaints that included – together with "class action" – the following search terms:

- "data security," "data privacy," or "data 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

- the words "collect" or "share" at a reasonable distance from the words "personal," "consumer," or "customer" at a reasonable distance from the words "zip," "address," "email," or "number"

- "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.*, "Deep Root Analytics" 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 Leighton Paisner'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.

AUTHORS

David Zetoony is the leader of Bryan Cave Leighton Paisner'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 Leighton Paisner LLP
Boulder, CO / Washington D.C.
David.Zetoony@bclplaw.com
202-508-6030

Jena Valdetero is the co-leader of Bryan Cave Leighton Paisner'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 Leighton Paisner LLP
Chicago, IL
Jena.Valdetero@bclplaw.com
312-602-5056

Andrea Maciejewski is a recent graduate of the University of Colorado at Boulder school of law and will join the firm as an associate in September 2019.

Bryan Cave Leighton Paisner LLP

With over 1,400 lawyers in 31 offices across North America, Europe, the Middle East and Asia, Bryan Cave Leighton Paisner LLP is a fully integrated global law firm that provides clients with connected legal advice, wherever and whenever they need it. The firm routinely defends clients in private litigation and regulatory enforcement actions involving data security breaches, and has assisted in over 600 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 Leighton Paisner's distribution list by clicking here.

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