

## Beyond Standing: Economic Experts In Breach Class Actions

*Law360, New York (May 14, 2015, 10:11 AM ET) --*

The recent experience of Anthem Inc., a large insurer, highlights some of the emerging trends in data breach litigation. Less than a day after Anthem made the announcement that personal health information and other personally identifiable information of as many as 80 million of its customers were compromised by hackers, a class action complaint was filed accusing Anthem of failing to protect its customers.[1] The speed with which the complaint was filed was not in and of itself unprecedented; many of the companies recently suffering data breaches have faced a class action complaint in the days following the announcement of a breach. Rather, the ubiquity of these filings (combined with the speed) is indicative of plaintiffs' view that the class action mechanism is best suited to litigating these (and future) data breach cases.



Mike Kheyfets

The early debate about data breach class actions focused on whether plaintiffs have standing under Article III of the U.S. Constitution, i.e., whether plaintiffs can show that they have suffered injury that is causally related to the alleged conduct. However, as injury theories have evolved, such cases have begun moving successfully past the standing stage.[2] As these cases proceed, then, an evaluation will need to be made by courts as to whether the proposed classes can be appropriately certified under Rule 23 of the Federal Rules of Civil Procedure. Among other issues, courts will need to evaluate in these proceedings whether “questions of law or fact common to class members predominate over any questions affecting only individual members.”[3]

### Role of Economic Experts in a Data Breach Class Actions

Expert economic testimony is an important component of many types of class actions and likely will gain similar prominence in data breach matters as those cases move to the class certification stage. This type of testimony provides context (and in some cases, direct proof) of liability and damages issues. An economic expert witness assists the trier of fact in understanding the evidence and provides objective, independent testimony on the economic impact of the alleged conduct. Experts are frequently employed in at least three phases of a class action, including class certification, liability, and damages.

In the class certification phase, the plaintiffs have the burden of proving that the same “common methodology” can be used to demonstrate that each potential class member was harmed by the alleged

conduct and that damages can be calculated on a formulaic basis.[4] At this stage, the economic expert provides testimony regarding the nature of the economic evidence and whether it can be applied to all class members collectively or, instead, must be considered on an individualized basis.

### **Expert Witness Approach to Class Certification Issues**

As part of their complaint, plaintiffs identify what they believe to be illegal conduct and define the class of individuals (or entities) that they allege were harmed by the conduct. In this type of case, the role of an economic expert is to analyze whether the empirical evidence can be used to show that all the members of the class, as defined, are sufficiently similar as to make the class action tenable. To assist in the review of class issues, the expert will typically make use of documents, deposition testimony, as well as analyses of breached and other data.

The purpose of the expert's assessment at this stage is to evaluate the proposed theories of harm in the context of the composition of the proposed class. That is, given class members' characteristics, is it in fact the case that all (or, in some cases, virtually all) could have suffered injury from the alleged conduct? Or, to the contrary, could (or did) some members avoid injury? Furthermore, can answers to these questions be determined by evidence common to the class, or would individualized inquiries be required? Similar questions with respect to damages must also be addressed by the expert at this stage. That is, the expert must evaluate whether — given the proposed theories of harm and the defined class — damages could be calculated using a formulaic approach. If they cannot, it may be the case that the class action mechanism does not fit the facts of the specific case.

The answers to these questions are case-specific and ultimately serve as guidance for the finder of fact as to whether the proposed class should be certified and the litigation should proceed. However, there is substantial precedent from class actions in other areas (e.g., *Comcast v. Behrend* in antitrust, *Wal-Mart v. Dukes* in employment, *Brazil v. Dole Food Company* in consumer protection, among many others) which dictates a rigorous expert review of these issues at the class certification stage. As data breach cases proceed to the class certification stage, equally rigorous expert analyses will be required in order to help the court make an appropriate determination.

### **A Selection of Claims and Damage Theories in Anthem**

Although at least 17 class actions related to the Anthem breach have been filed,[5] there exists substantial overlap between the complaints on the proposed damages theories. For example, the complaint filed in the Central District of California states that “the information Defendants lost, including Plaintiff's PII and PHI, is ‘as good as gold’ to identity thieves.”[6] Plaintiffs in that case have alleged that identity thieves can use the information accessed during the breach to:[7]

- “open new financial accounts and incur charges in another person's name, take out loans in another person's name, incur charges on existing accounts, or clone ATM, debit, or credit cards.”
- “perpetrate a variety of crimes that do not cause financial loss, but nonetheless harm the victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.”

- “get medical services using the Plaintiff’s PII and PHI or commit any number of other frauds, such as obtaining a job, procuring housing, or even giving false information to police during an arrest.”

The California plaintiffs have defined the class as including “all persons [...] whose personally identifiable information, personal health information, and/or financial information was breached as a result of the data breach announced on or about February 4, 2015,” a number they believe “is in the millions.”[8] They have further claimed that the putative class members have “suffered injury in fact and lost property and money as a result of Defendants’ conduct.”[9]

Similarly, the complaint filed in the Northern District of Alabama identifies “at least 80 million class members”[10] that are “current or former customers of Anthem, Inc. and its subsidiaries and/or affiliates and whose PII/PHI was wrongfully accessed, copied, and transferred between the time period of January 1, 2014 and February 5, 2015.”[11] Plaintiffs in this case have alleged several types of harm, including:

- “[A] substantially increased risk of additional instances of identity theft and resulting losses.”[12]
- “[Expenditure of] significant time and money to protect themselves; including, but not limited to: the cost of responding to the data breach, cost of conducting a damage assessment, costs to obtain credit reports, costs to obtain future credit reports, cost for credit monitoring, costs for insurance to indemnify against misuse of identity, costs to rehabilitate Plaintiff’s and Class Members’ PII/PHI, and costs to reimburse from losses incurred as a proximate result of the breach.”[13]
- “[Loss of value resulting from] the difference between the price Plaintiff and the Class paid in reliance upon Defendant’s duty/promise to secure its members’ PII/PHI, and the actual services — devoid of proper protection mechanisms — rendered by Defendant.”[14]

### **Economic Analysis of Proposed Claims**

Although the claims described above are only a sampling of those made in the 17 class actions brought against Anthem, their variety — as well as the sizes of the proposed classes — underscore the importance of rigorous expert analysis at the class certification stage. That is, when a proposed class is made up of tens of millions of individuals — with each individual harmed in a number of ways — the certification of that class rests crucially on the plaintiffs’ expert’s ability to design a model capable of determining whether all (or, in some cases, virtually all) class members could have suffered injury from the alleged actions.

Consider, for example, the alleged harm to class members resulting from the “difference between the price Plaintiff and the Class paid in reliance upon Defendant’s duty/promise to secure its members’ PII/PHI, and the actual services — devoid of proper protection mechanisms — rendered by Defendant.”[15] To the extent class members purchased different products from Anthem, or even the same product but at various prices, the difference (if any) that the plaintiffs claim resulted from the breach may not be common to the class. Moreover, to the extent Anthem’s prices did not contain an explicit “data security” component, the loss of value (if any) for a given customer resulting from the breach would be inherently individualized. Ultimately, the plaintiffs’ burden would be to propose a

method that would be able to evaluate whether the claimed harm (as well as all the other proposed types of harm) from the alleged conduct can be evaluated on a classwide basis. If the method is unable to do so for all (or virtually all) class members, certification of the proposed class may not be appropriate.

—By Mike Kheyfets, Edgeworth Economics LLC

*Mike Kheyfets is a partner in Edgeworth Economics' Washington, D.C., office.*

*The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.*

[1] <http://www.law360.com/articles/618932/anthem-hit-with-class-actions-following-data-hack>

[2] <http://www.hldataprotection.com/2014/12/articles/privacy-security-litigation/courts-split-on-standing-for-consumer-plaintiffs-in-data-breach-class-actions/>

[3] Rule 23(b)(3), Federal Rules of Civil Procedure.

[4] Rule 23(a), Federal Rules of Civil Procedure.

[5] These include seven cases in Indiana, five in the Central District of California, and one each in the Eastern and Northern Districts of California, the Northern District of Alabama, the Southern District of Ohio, and the District of Georgia. Plaintiffs have also moved to consolidate all 17 cases in Indiana. (See <http://www.law360.com/privacy/articles/620833>)

[6] Kirby v. Anthem, Inc. et al, Class Action Complaint, February 5, 2015, (“Kirby Complaint”), ¶23.

[7] Kirby Complaint, ¶¶24-27.

[8] Kirby Complaint, ¶¶33-34.

[9] Kirby Complaint, ¶47.

[10] Juliano v. Anthem, Inc., Class Action Complaint, February 5, 2015, (“Juliano Complaint”), ¶36.

[11] Juliano Complaint, ¶34.

[12] Juliano Complaint, ¶7.

[13] Juliano Complaint, ¶14.

[14] Juliano Complaint, ¶125.

[15] Juliano Complaint, ¶125.