Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Obstacles To Defining Injury, Class In Cyberattack Suits

By **Michael Kheyfets** (June 9, 2021, 2:06 PM EDT)


Michael Kheyfets

Courts' decisions on whether a particular class of plaintiffs should be certified often turn on a combination of factors, including the reliability of proposed economic models, the nature of offered representative evidence, and the prevalence of uninjured members.

The issue of uninjured class members — and in particular, the question of whether the need to quantify and identify those class members predominates — has grown increasingly central to the class certification inquiry.

While this question is pertinent across different types of class action claims, the relevant economic analysis of it is potentially most novel in the area of data privacy litigation.

Cyberattacks are continuously evolving, as are the legal claims stemming from those attacks and the analysis necessary to assess those claims. Whereas even a few years ago, many data privacy cases would be resolved before the class certification stage, it is increasingly common to see these issues briefed and examined.

As economists are increasingly asked to study questions of impact and damages in data privacy cases, it is important that those studies are based on a proper understanding of the relevant legal frameworks.

Economic models will need to evolve as well, such that they not only purport to provide average or aggregate measures of harm, but also have the ability to reliably assess the prevalence of potentially uninjured class members.

As I discuss in this article, as economic and legal analysis in data privacy litigation continues to mature, guidance from areas with more mature histories of jurisprudence may be probative.

Defining "Uninjured Class Members"

In the area of antitrust class actions — which has a long history of jurisprudence — economists think of potential class members as being injured if they paid higher prices for the product at issue than they would have paid in a world where the alleged conduct did not occur (known as the but-for world).

Conversely, an uninjured class member would be one who did not pay an elevated price relative to a reliably estimated but-for world.

While the economic analysis in antitrust cases can be quite complex, and often relies on statistical modeling such as regression analysis, the unit of injury tends to be straightforward — i.e., a price paid for a product at issue.

But in data breach class actions — where claims usually center around unauthorized access and/or disclosure of plaintiffs' sensitive information — even such a fundamental question may not be so clear.

This is because plaintiffs in consumer data breach cases often offer a variety of disparate theories of harm. Depending on the nature of the breach, offered theories may include a combination of the following (among others):

- Fraudulent payment card charges or money stolen from bank accounts using disclosed financial information;
- Lost opportunity costs associated with the effort expended addressing (and attempting to mitigate) the actual and future consequences of the data breach;
- Fees related to exceeding payment card limits, balances and bounced transactions;
- Harm resulting from damaged credit scores and information; and
- Out-of-pocket expenses associated with the prevention, detection and recovery from identity theft, tax fraud and/or unauthorized use of personally identifiable information, or PII.

Developing a common economic model capable of assessing injury across such varied offered theories presents a threshold challenge for plaintiffs seeking to certify a class. However, determining whether any model offered by plaintiffs is capable of quantifying and identifying uninjured class members makes the inquiry even more challenging.

Defining "Uninjured Class Members" in a Data Breach Litigation

Consider what it may mean for a potential class member to be economically uninjured under a given set of theories of harm. For example, this could include anyone whose information was disclosed in a breach, but who:

- Did not incur fraudulent charges or did not have money stolen from bank accounts;
- Did not engage in efforts to address the consequences of the data breach (and thus had no lost opportunity costs);
- Did not incur fees related to exceeding payment card limits;
- Did not suffer damage to credit scores; or
- Did not have his or her identity used fraudulently and thus did not incur out-of-pocket expenses associated with the prevention, detection and recovery from identity theft.

The economic studies plaintiffs offer to assess the questions of impact and damages vary in scope and substance, but all generally rely on what is called representative evidence — i.e., evidence meant to represent the experiences of absent class members, rather than data on their actual experiences.

The consideration of whether representative evidence in theory could be used to satisfy predominance is a different one than whether — given a particular set of facts and evidence — it in fact does (or whether it masks relevant individualized differences).

The issues of uninjured class members and representative evidence directly intersect in data breach matters.

It is often the case that the proposed economic analyses rely on the results of published surveys and other studies not specifically related to the litigation at issue.

Such studies may indicate that, on average, victims of a data breach may suffer a certain amount of fraudulent payment card activity, or spend a certain amount of time and money addressing the consequences of the data breach, or sustain a certain decline in their credit scores.

Such aggregate evidence, however, would be unable to determine the prevalence of uninjured members in a given proposed class, or to identify them individually.

For example, a published survey may provide aggregate statistics on the average amount of credit card fraud per consumer, or the amount of time and money the average individual may be willing to devote to preventing identity theft. However, it cannot determine how many individuals in a given class — i.e., tied to a specific data breach — suffered any of the alleged harms, and how many did not (and were thus uninjured).

Unique Considerations in Data Breach Litigation: Increased Risk of Future Harm

An element of data breach cases that further complicates the class certification analysis is that plaintiffs often claim the breach has not just caused actual injury, but that disclosure of their PII has caused an increased risk of future harm. That is, such theories claim that because stolen information need not be fraudulently misused immediately, plaintiffs risk injury that has not yet occurred at the time their case was filed.[1]

The debate is ongoing as to whether an increase in the risk of future harm confers standing under Article III of the U.S. Constitution.[2]

However the issue of uninjured class members looms here as well. That is, not only would plaintiffs seeking to certify a class under a future harm theory need to offer economic models capable of assessing impact on a classwide basis, but these models would need a mechanism by which to rule out the possibility that class members would remain uninjured in the future as well.

Ransomware Attacks: Considerations for Alleged Injury Due to Supply Chain Interruption

While the more typical data breach class action involves claims related to unauthorized access and/or disclosure of plaintiffs' own sensitive information, the recent Colonial Pipeline Co. ransomware attack represents a different cybersecurity — and litigation — risk for companies.

This attack was launched on May 6 by Eastern European hackers who locked Colonial's computers with ransomware, which in turn resulted in Colonial shutting down its fuel distribution pipeline. The fallout — increased gas prices[3] and panic buying[4] — dominated the headlines.

Colonial's pipeline operation resumed less than a week later on the evening of May 12,[5] and the first class action related to this attack was filed in the U.S. District Court for the Northern District of Georgia less than a week after that.[6] The case is Ramon Dickerson v. CDPQ Colonial Partners LP.

The fact of the Colonial attack was not necessarily novel. For example, a recent study by insurer Hiscox Inc. found that nearly half of businesses in Europe and North America were targeted by cybercriminals in 2020, and one in six cyberattacks used ransomware.[7]

And in Dickerson, the plaintiffs' allegations that the "Defendant's failure to adequately protect their systems from the aforementioned ransomware attack"[8] also echoed those in other data breach cases.

However, the novelty of the Dickerson case lies in the theory of economic harm. Specifically, the plaintiffs allege that inadequate data security caused "gas shortages and increased prices for gasoline purchased by consumers and other end-users."[9]

They are seeking to certify a class of "all entities and natural persons who purchased gasoline from May 7, 2021, through Present and who paid higher prices for gasoline as a result of the Defendant's conduct."[10]

The Dickerson plaintiffs' claim turns the uninjured class member issue on its head by defining a fail-safe class — i.e., one that cannot be defined until the case is resolved on its merits.[11]

That is, by definition, the proposed class only includes consumers who were injured because they "paid higher prices for gasoline as a result of the Defendant's conduct," as opposed to a broader set of "all entities and natural persons who purchased gasoline," and does not include anyone who was uninjured.

However, from an economic perspective, there are challenges to analyzing this kind of claim in the standard counterfactual framework — i.e., comparing actual and but-for prices — using a purportedly common model.

One issue is the breadth of the proposed class. For example, the Colonial Pipeline supplies about 45% of the fuel consumed on the East Coast,[12] which represents thousands of gas stations across a broad geographic region.

Given the localized nature of competition among retail gasoline sellers,[13] it is likely that the assessment of whether any proposed class member paid a price that was higher than a reliably estimated but-for price will require analysis of localized economic conditions.

Another potentially relevant issue relates to individual class members' purchasing patterns. Given public reports of panic buying and hoarding,[14] it would be relevant to assess whether proposed class members potentially induced injury by knowingly buying gasoline at elevated prices rather than mitigating some (or all) harm by waiting for any potential effects of the attack to abate.

Given these issues, the application of representative evidence weighs on the analysis in the ransomware

cases as well. While aggregate pricing and consumer behavior data may inform the question of average trends, these factors would be unable to define the scope of the proposed class — i.e., distinguish consumers that paid elevated prices "as a result of the Defendant's conduct" from those that did not.

For example, it would not be possible to use aggregated trends to identify gas stations that did not raise prices as a result of the alleged conduct (instead choosing to sell out of existing inventories at preattack prices).

The Colonial Pipeline ransomware attack may provide a blueprint for hackers seeking to profit from disrupting key supply chains. For example, less than a month after the Colonial attack, JBS SA — the world's largest meat processor — was targeted by a ransomware attack.[15]

However, many open questions remain about the viability of consumers' elevated price claims stemming from such attacks, as well as the amenability of those claims to class treatment.

Michael Kheyfets is a partner at Edgeworth Economics LLC.

[1] For example, such theories may posit that plaintiffs will incur future costs in terms of time and money to prevent or remedy the effects of fraud using their PII.

[2] https://www.reuters.com/article/us-otc-databreach/in-major-ruling-2nd-circuit-says-no-circuit-split-on-data-breaches-and-standing-idUSKBN2CD2I4.

[3] https://www.reuters.com/business/energy/us-pump-prices-head-highest-since-2014-hacked-fuel-pipeline-shut-2021-05-10/.

[4] https://www.washingtonpost.com/business/2021/05/13/gas-stations-await-relief-panic-buyers-while-colonial-pipeline-restores-service/.

[5] https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/colonial-pipeline-investigation/.

[6] Dickerson v. CDCP Colonial Partners, L.P., Case No. 1:21-cv-02098 (N.D. Ga.).

[7] https://www.law360.com/articles/1376896/almost-half-of-firms-hit-by-cyberattack-in-2020-report-says.

[8] Dickerson v. CDCP Colonial Partners Class Action Complaint, May 18, 2021 ("Dickerson Complaint"), ¶39.

[9] Dickerson Complaint, ¶39.

[10] Dickerson Complaint, ¶47.

[11] https://attorneyatlawmagazine.com/fail-safe-classes.

[12] https://www.wsj.com/articles/colonial-pipeline-cyberattack-hack-11620668583.

[13] http://faculty.haas.berkeley.edu/giyer/index_files/GaneshSeethu_QME_March2008.pdf; https://ideas.repec.org/a/mve/journl/v36y2010i2p75-97.html; https://www.usi.edu/media/3654786/Competition-and-Cooperation.pdf.

[14] https://www.cbsnews.com/news/gas-prices-colonial-pipeline-shutdown-panic-buying-hoarding-long-lines-outages/.

[15] https://www.law360.com/cybersecurity-privacy/articles/1389817/ransomware-disrupts-operations-at-global-meatpacker-jbs?.