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

Data Breach Class Actions: Addressing Future Injury Risk

By **Robert Kriss and Jerel Dawson, Mayer Brown LLP**

Robert Kriss

Jerel Dawson

Law360, New York (May 16, 2017, 12:22 PM EDT) -- Recently, the Eighth Circuit vacated an order approving a settlement in a data breach class action and remanded the case to the district court with instructions to address whether the interests of absent class members whose personal information had not been misused were adequately considered in approving the settlement. In re: Target Corporation Customer Data Security Breach Litigation, 847 F.3d 608 (8th Cir. 2017). The court of appeals asked the district court to consider whether an intraclass conflict existed between class members whose personal information had been misused and those whose information had not been misused as of the date of the settlement, and whether the conflict required certification of one or more subclasses with independent representation, or could be adequately addressed in some other fashion.

A defendant considering settling a case generally will be willing to enter into a settlement only if all the claims of class members are released with finality in exchange for the settlement consideration, subject to an acceptable number of class members opting out of the settlement. The Eighth Circuit opinion raises questions that could affect the finality and cost of settlements and, accordingly, whether and how a data breach class action can be settled.[1]

Subclasses are required only when there is a "fundamental" intra-class conflict. Such a conflict exists, for example, when groups have to take different substantive positions on a specific issue in the case; when one group's establishing its claims has the necessary impact of diminishing another group's claims; or when there is reason to believe that the total amount of recovery is fixed and different groups have claims of arguably different strength, which affects the formula for allocating a settlement fund to various groups of plaintiffs. See, e.g., Dewey v. Volkswagen Aktiengesellschaft, 681 F.3d 170, 184 (3d Cir. 2012).

As the court in Dewey explained: "A fundamental conflict exists where some [class] members claim to have been harmed by the same conduct that benefited other members of the class." 681 F.3d at 184 (quoting

Valley Drug Co. v. Geneva Pharmaceuticals Inc., 350 F.3d 1181, 1189 (11th Cir. 2003)). A conflict is fundamental where it touches 'the specific issues in controversy.' [citations omitted] A conflict concerning the allocation of remedies among class members with competing interests can be fundamental and can thus render a representative plaintiff inadequate. [citations omitted] A conflict that is unduly speculative, however, is generally not fundamental. [citations omitted]"

The objector in the Target case has argued that there is a fundamental conflict between class members who have suffered a misuse of their data as of the date of the settlement and those who have not because those who have suffered misuse have damage claims that those who have not yet suffered misuse do not. At the same time, the objector asserts that all class members are exposed to the risk of future misuse and that most of the persons involved in the data breach have not yet suffered misuse.

We believe the objector's objection is based upon a misunderstanding of the implications of the facts he asserts in his objection. When a data breach occurs involving personally identifiable information that can be used to commit identity theft, persons involved in the breach can suffer identity theft in the future, although the available information suggests that typically a very small percentage of persons involved will suffer any misuse of their information. See, e.g., Beck v. McDonald, 848 F.3d 262, 275, 276 (4th Cir. 2017) (plaintiff alleges that 33 percent of those affected by breach will suffer identity theft; court concludes probability is too low to establish standing). Even class members who have suffered one instance of identity theft as of the filing of the complaint conceivably could suffer additional instances of identity theft after the filing of the complaint and after the settlement is consummated. Therefore, all persons involved in a data breach are similarly situated with respect to a future identity theft, whether they have suffered misuse at the time of the settlement or not.

Target involved theft of credit card information, not Social Security numbers. Therefore, it is difficult to see how the breach in Target could result in the type of identity theft where a bad actor is able to open new accounts or receive payments, such as tax refunds, using the victim's identity. Misuse of the information in Target most likely would be limited to making false charges on a credit card, and the risk of future injury would terminate if and when the credit card number was changed. The risk of future identity theft involving the opening of new accounts or diversion of payments is somewhat greater when other personally identifiable information such as Social Security numbers is acquired in the breach, although that risk can be mitigated by requesting a credit freeze or fraud alert from the credit reporting services (see identitytheft.gov).

In either case, a class member whose personal information was misused to commit credit card fraud or identity theft will have an incentive to negotiate for reimbursement of costs he incurred up to the date of the settlement to minimize his risk of credit card fraud or identity theft after the settlement. Potential future losses occurring after the settlement are speculative and should not be deemed to create the kind of fundamental conflict with the class that requires subclasses. The right to opt out of the settlement should be sufficient protection for class members who have not experienced a misuse of their information before the consummation of the settlement and wish to preserve their speculative claims rather than claim the monetary relief provided by the settlement.

The objector in Target argues that the U.S. Supreme Court in Amchem Products Inc. v. Windsor, 521 U.S. 591 (1997), and Ortiz v. Fibreboard Corp., 527 U.S. 815 (1999), has held that there always is a fundamental conflict between class members who have suffered a present injury and those who may suffer a future injury (in those cases, illness and the risk of illness from exposure to asbestos). However, the objector fails to recognize important factual distinctions between the asbestos cases and data breach cases.

In the asbestos cases, the class members who were ill at the time of the settlement have accrued claims to obtain an adequate remedy and no need, and therefore no incentive, to consider the interests of those who are not yet ill. In contrast, as discussed above, all class members in a data breach case involving information that could be used to commit identity theft have an interest in receiving compensation for costs incurred before consummation of the settlement to minimize the risk of identity theft after the settlement, whether or not they have suffered an instance of identity theft before the consummation of the settlement. See, e.g., Dewey, 681 F.3d 170 (distinguishing Amchem and Ortiz from the case at issue where class representatives whose automobile sunroofs started leaking before the settlement could experience new leaks after the settlement and therefore had an adequate incentive to represent the interests of those class members whose sunroofs had not started to leak prior to consummation of the settlement).

In determining whether subclasses are required and whether a settlement and release of claims is fair and reasonable to all members of the class, it is appropriate to compare outcomes in a settlement scenario to potential outcomes if the case were not settled. Cf., National Super Spuds Inc. v. N.Y. Mercantile Exchange, 660 F.2d 9, 17-18 (2d Cir. 1981) (determining the fairness of the scope of a release in a settlement agreement by considering possible outcomes if the case had been litigated on the merits). This analysis further supports the reasonableness of not creating subclasses in data breach class action settlements or evaluating the fairness of the settlement based upon impact on different groups of plaintiffs.

If a class were certified in a data breach class action and none of the claims involved an award of statutory damages, individual plaintiffs who had not opted out of the class action prior to the damage phase of the proceeding would have to submit and prove their individual claims in a damage phase, and the defendant would have an opportunity to rebut the individual plaintiffs' evidence. See, e.g., Smith v. Triad of Alabama LLC, No. 1:14-CV-324-WKW, 2017, at *16 (M.D. Ala. March 17, 2017) (certifying a consumer class in a contested data breach class action: "If Plaintiffs prevail, the intermingled questions of causation and damages will then be tried on an individual basis"). If the absent class member did not opt out and did not have a cognizable claim by the time of the damage phase of the proceeding, or if the absent class member was not interested in prosecuting his or her individual claim, the absent class member's claim would be barred with finality at the end of the proceeding.

This litigation scenario strongly supports not creating subclasses of persons who have not suffered misuse of personal information in a data breach or separately considering their objections to the fairness of a settlement. Allowing class members to opt out of the class action settlement results in an outcome for them that is at least as favorable, if not more favorable, than if the case were decided on the merits through the damages phase.[2]

With a proper understanding of the nature of data breaches and their potential future impact upon all members of the class, it is apparent that there is no fundamental conflict among persons involved in a data breach. Proceeding with a single class in considering the fairness of a settlement, and allowing class members to opt out of the settlement, adequately protects the interest of all class members and is completely consistent with what would happen if the case were not settled but instead was tried on the merits.

Robert J. Kriss is a partner and Jerel D. Dawson is an associate at Mayer Brown LLP in Chicago.

[1]Although not mentioned in the Eighth Circuit opinion, there is a threshold issue concerning the ascertainability of members of subclasses that is relevant to whether subclasses or any class should be certified in a data breach case where some putative class members have suffered injury as a result of misuse of their information and others have not. Identification of persons falling within those categories would require individualized mini trials. There currently is a split among the circuits as to whether ascertainability is a requirement for class certification and, if so, the standard that should be applied. See Archis A. Parasharami & Daniel Jones, Ninth Circuit rejects meaningful ascertainability requirement for class certification, cementing deep circuit split, Mayer Brown Class Defense Blog, Jan. 6, 2017, https://www.classdefenseblog.com/2017/01/ninth-circuit-rejects-meaningful-ascertainability-requirement-class-certification-cementing-deep-circuit-split/; compare EQT Prod. Co. v. Adair, 764 F.3d 347, 358 (4th Cir. 2014) ("[I]f class members are impossible to identify without extensive and individualized fact-finding or 'mini trials,' then a class action is inappropriate."); with Mullins v. Direct Digital LLC, 795 F.3d 654, 658 (7th Cir. 2015) ("Nothing in Rule 23 mentions or implies this heightened requirement under Rule 23(b)(3), which has the effect of skewing the balance that district courts must strike when deciding whether to certify classes."). For purposes of this article, we will assume that ascertainability is not an obstacle to certifying a class, at least for settlement purposes. Also, we are not commenting on whether a class could properly be certified in a contested data breach case. In this article, we address only a settlement scenario.

[2] There also is no need to create subclasses to address the fairness of any injunctive component of a data breach class action settlement. First, it should be noted that some courts have held that parties injured by a past data breach do not have standing to seek an injunction to prevent a future data breach. See Beck, 848 F.3d at 277-78 ("The most that can be reasonably inferred from the Plaintiffs' allegations regarding the likelihood of another data breach at Dorn VAMC is that the Plaintiffs could be victimized by a future data breach. That alone is not enough."). In any event, injunctive relief is based upon Rule 23(b)(2) of the Rules of Civil Procedure, which does not allow class members to opt out. In a litigation or settlement scenario, the decision of an adequate class representative with respect to injunctive relief binds all members of the class. A class representative who has suffered a misuse of his

information has the same interest as a person who has not yet suffered a misuse of her information in preventing a future data breach that could result in further disclosure of their information. Therefore, with respect to any injunctive component of a data breach class action settlement, there should be no need to create a subclass of persons who have not suffered a misuse of their information. The injunctive relief, if any, accepted by the class representative as part of the settlement should be final as to all class members, including those who opted out to preserve their damage claims.