Published on *The National Law Review* https://natlawreview.com

No Happy Hour Here: $7.1 Million Settlement Reached in Alcohol Delivery Data Breach Class Action Litigation, Class Members Anticipated to Get $14 Cash Payout

Article By:

Kristin L. Bryan

Data breaches are on the rise, and with a rise in breaches comes an accompanying increase in data breach litigation. A recent class action settlement involving the largest online alcohol marketplace in North America, with retail partners in more than 1,400 cities, underscores how all companies across industries are impacted by this trend.

First, let's look at the (alleged) facts. Drizly is a company that operates an online e-commerce platform that facilitates the delivery of alcoholic beverages from local retailers. The litigation, *Barr v. Drizly, LLC*, Case No. 1:20-cv-11492 (D. Mass.), concerned a data event which Plaintiffs allege resulted in consumers' information, including at least email addresses, dates of birth, hashed passwords, delivery addresses, phone numbers, and IP addresses, to be improperly exposed to third parties on the dark web. The data event was allegedly the result of a targeted attack that occurred around February 2020 but was not identified by Drizly until the end of July 2020.

Plaintiffs sought to certify a putative class and asserted claims against Drizly for negligence, negligence *per se*, breach of implied contract, unjust enrichment, and various consumer protection claims under the laws of Massachusetts, New York, Arizona, and California. After Plaintiffs amended their Complaint in October 2020, Drizly moved to compel arbitration. This was on the basis that before using Drizly to order alcohol, users must register for an account and agree to Drizly's Terms. Those Terms disclose, in all capital letters at the top of the page, that users agree to resolve any disputes through individual arbitration. Based on the Federal Arbitration Act, which reflects a liberal federal policy favoring arbitration, Drizly argued the arbitration provision precluded the Plaintiffs' lawsuit.

However, before the court ruled on Drizly's motion, the parties reached a preliminary settlement (subject to court approval). This agreement defines a Settlement Class, consisting of "All Persons in the United States whose customer data was compromised in the data intrusion security incident that Drizly made public on July 28, 2020, in which an unauthorized party accessed certain personally identifiable information of Drizly's customers."

Under the terms of the settlement, each eligible Class Member that files a timely and valid Proof of Claim and Release ("Claim Form") will receive an individual cash payment of ***$14.00***, that may be

adjusted upward if the total amount due to all Authorized Claimants does not exceed $1,050,000, and adjusted downward in the event that the aggregate cash payments to all Authorized Claimants exceeds $3,150,000. Additionally, as Plaintiffs outlined to the court, Class Members will also receive a pro rata portion of a pool of up to $447,750 in the form of a credit against the cost of service fees for future orders from Drizly. Finally, Drizly will also implement and maintain for a two-year period certain dtat

What explains this result? To put it simply, uncertainty in this area of the law and the high cost of continued litigation.

Plaintiffs conceded in their submission to the court asking for settlement approval that "[w]hile Plaintiffs believe they would have prevailed, there are risks involved in data breach litigation—a relatively new area of law—including proving standing and causation." ECF 52-1 at 15 (citing *In re Tyco Int'l, Ltd. Multidistrict Litig.*, 535 F. Supp. 2d 249, 260 (D.N.H. 2007) (noting that, because the case "involved a greater risk of non-recovery" due to "still-developing law," this factor weighed in favor of approval); *see also In re Sonic Corp. Customer Data Sec. Breach Litig.*, No. 1:17-md2807, 2019 WL 3773737, at *7 (N.D. Ohio Aug. 12, 2019) ("***Data breach litigation is complex and risky. This unsettled area of law often presents novel questions for courts***.") (emphasis added).

Additionally, Plaintiffs also conceded that they "likely would have incurred significant costs to prove their case through fact and expert discovery." ECF 52-1 at 15 (citing *In re Yahoo! Inc. Customer Data Security Breach Litig.*, No. 16-MD02752, 2020 WL 4212811, at *9 (N.D. Cal. July 22, 2020) (listing "more discovery" as one of the significant expenses for continuing a data breach litigation); *see also In re Compact Disc Minimum Advertised Price Antitrust Litig.*, 216 F.R.D. 197, 212 (D. Me. 2003) (explaining that, absent settlement, "[m]ore experts will have to be hired at great expense")).

The court overseeing the case has granted preliminary approval of the settlement, with notice currently underway to class members. A final approval hearing has been scheduled for later in the year.

Another day, another data breach litigation (most likely) resolved early on. Will this trend continue? Only time will tell. Not to worry, CPW will be there to keep you in the loop. Stay tuned!

National Law Review, Volume XI, Number 137