October 2016

US CLASS ACTIONS FILED IN WAKE OF YAHOO HACK DISCLOSURE

As has been widely reported, Yahoo announced on September 22, 2016 that it had suffered a hack in 2014 that compromised customer information relating to 500 million user accounts, approximately half of all accounts Yahoo maintains. As has become common, this revelation was swiftly followed by class action lawsuits commenced in the US on behalf of users whose information may have been stolen. The three complaints filed to date allege claims based on a wide array of legal theories, but share certain common obstacles to success.

Cases Are Filed Immediately, Including Outside Yahoo's Home Court

Plaintiffs' counsel wasted no time, filing two actions in US federal courts on the very day a breach was announced, and a third the following day, each seeking the certification of a nationwide plaintiff class of those whose information was accessed by Yahoo's hackers, as well as state-specific subclasses for certain claims under state law. More cases can be expected as new developments are reported.

While Yahoo is US-based, only one action (*Schwartz v. Yahoo! Inc.*) was filed in the US District Court for the Northern District of California, where Yahoo has its headquarters. The other two cases, *Myers v. Yahoo! Inc.* and *Havron v. Yahoo, Inc.*, were filed in the Southern District of California and the Southern District of Illinois, where the respective plaintiffs reside. Although the allegations of jurisdiction over Yahoo in the complaints are conclusory, Yahoo is unlikely to move to dismiss on the basis of personal jurisdiction, as it is well settled that jurisdiction may be established over a

company that targets residents of the state in offering services over the internet.

The three complaints assert a wide array of claims under state common, statutory and constitutional law. Although there is only one claim asserted under federal law (*Myers* contains a claim under the Stored Communications Act), plaintiffs are proceeding in federal court under the Class Action Fairness Act, which allows large class actions to be brought in federal court if some members of the class reside in a different state than the defendant. The primary legal theories are: (1) breach of express or implied contract, (2) negligence or gross negligence, (3) unfair business practices and (4) violation of privacy rights under the common law and California constitution.

Yahoo Has Substantial Defenses

Regardless of the legal theory asserted by the plaintiffs, they all face significant common obstacles to proceeding with their claims, both at the initial motion to dismiss stage and in certifying a class.

First, as a matter of federal constitutional law, US federal courts can only hear claims if the plaintiff has sufficient standing to bring them. As the United States Supreme Court recently held in *Spokeo Inc. v. Robins*, 136 S. Ct. 1540 (2016), a plaintiff must have experienced or be imminently likely to experience harm (an "injury-in-fact") that is concrete—the mere fact that a violation of law has occurred is not actionable unless it has hurt or is about to hurt the plaintiff in a tangible way. Here, none of the plaintiffs can even be sure his or her account was among those accessed, and none has suffered identity theft or fraudulent charges, though the plaintiff in *Schwartz* has paid to put a security freeze on his credit profile. Instead, they simply conclusorily allege that other members of the class have suffered such losses and that all are at greater risk. The exposure of personal information and risk of identity theft repeatedly have been held to be insufficient to establish standing in data breach cases, and paying for a credit monitoring service or security freeze cannot manufacture standing if the risk of misuse of the information is unproven. Although the California courts are in the Ninth Circuit and the Court of Appeals there applies a less stringent test for standing in data breach cases, in the absence of any evidence that members of the class have in fact been victims of identity theft, plaintiffs will struggle to overcome a challenge to their standing.

Second, in seeking leave to proceed as class representatives, and ultimately requesting the certification of a class, a proposed lead plaintiff must establish, among other things, that his or her own claims are sufficiently typical of those of the class to be an appropriate representative of the class in the litigation. In this context, the *Schwartz* plaintiff's security freeze may be a factor in finding that he is not typical of the class; likely few class members have taken that protective measure and therefore the balance have a higher likelihood of suffering fraudulent charges or damage to their credit from identity theft.

Typicality may also be an issue in the information obtained about different class members. Yahoo's platform includes a number of different sites and services, including email, fantasy sports and the Flickr photo-sharing service. (Yahoo's website states that information on accounts on Tumblr, a blogging service it acquired n 2013, was not accessed.) The nature of the information submitted to open accounts for each platform may differ; for example, a person who played fantasy sports may have added credit card information, whereas a person simply setting up an email account may have provided incomplete or fictitious information. The degree of security required by Yahoo, and therefore the strength of the passwords used and whether security questions were required, also may have differed by service or by the security requirements when the user joined. Subsequent changes to security requirements will not have been implemented by users who stopped using their accounts. As a result, the hackers may have information of widely differing value depending on user behaviour, and a particular individual's risk of identity theft may not be typical of the class.

Finally, many of the causes of action in these cases are subject to dismissal because plaintiffs have failed to plead essential elements of their claims. For example, the claims for breach of contract and deceptive business practices rest on the contention that Yahoo promised to comply with federal regulations on the protection of its customer information and failed to do so. But the mere

fact of a breach does not fairly suggest, under the plausibility standard applicable in federal court, that Yahoo must have fallen short of those standards, nor have plaintiffs identified any particular regulation that Yahoo has failed to comply with.

But the Fight Probably Will Not Be Over Soon

The three cases that have already been filed represent only the opening salvos in litigation relating to the hack. These complaints are likely to be amended, and new complaints filed, as additional information available. New claims may be added under additional state laws on behalf of classes resident in those states. Even if some complaints are dismissed, others will try to new tactics to avoid dismissal—for example, plaintiffs may attempt to connect incidents of identity theft that have occurred since 2014 to the disclosure of their Yahoo credentials to bolster their standing based on concrete harm. If a substantial volume of cases are filed, they may be transferred to consolidate them in a particular district before a single judge to make them more manageable.

Key contacts

If you require advice on any of the matters raised in this document, please call Laura Hall or your usual contact at Allen & Overy.

Laura R. Hall
Partner
USA - New York

Contact
Tel +1 212 756 1171
laura.hall@allenovery.com

Allen & Overy LLP

One Bishops Square, London E1 6AD, United Kingdom

Tel +44 20 3088 0000

Fax +44 20 3088 0088

www.allenovery.com