image: Mina De La O / DigitalVision / Getty Images

Margaret Reetz Partner
margaret.reetz@mendes.com
Mendes & Mount LLP, New York

Yahoo! data breach litigation to proceed

On 9 March 2018, the United States District Court for the Northern District of California, San Jose Division, granted in part and denied in part Yahoo! Inc. ('Yahoo') and Aabaco Small Business, LLC's ('Aabaco') (collectively, 'the Defendants') motion to dismiss putative class litigation brought by nine named individuals ('the Plaintiffs') over the way the Defendants handled several data breaches that occurred between 2013 and 2016. The Court's decision has paved the way for the Plaintiffs' class action suit to proceed, and in this article, Margaret Reetz, Partner at Mendes & Mount LLP, dissects the Court's reasoning and both parties' grounds in the case.

"Yahoo! was founded in 1994," so begins the recent Court decision, which goes on to depict the considerable, then immense and, still more colossal "security failures" to befall Yahoo[1]. The numbers are staggering so, inevitably, class litigation ensued. Yahoo, like many a data breach defendant before it, sought to dismiss the class claims on various grounds, but the class will proceed with claims based on negligence, breach of contract, and misrepresentation, including punitive damages claims, amongst others.

A seemingly never ending breach saga

As detailed in the Court's recent ruling, Yahoo's corporate network was compromised in 2008 and 2009[2]. In 2010, Google notified Yahoo that attackers were using Yahoo systems to attack Google. In 2011, Yahoo's Chief Information Security Officer ('CISO') noted "gaping holes" in its security. In 2012, Yahoo was informed by outsiders of vulnerabilities, and also in 2012 Yahoo announced that a security breach had exposed 450,000 usernames and passwords[3]. The 2012 hack revealed that Yahoo failed to cryptographically store passwords in its database - the passwords were stored in plain text[4].

The three breaches

The customer class litigation involves three data breaches that occurred between 2013 and 2016. The first breach occurred in August 2013. Hackers gained access to Yahoo accounts and stole users' Yahoo logins, country codes, recovery emails, dates of birth, hashed passwords, telephone numbers and zip codes[5]. The 2013 breach also gave the attackers access to the contents of user emails, and thus exposed any sensitive information included in the email contents.

The Plaintiffs alleged this included credit card numbers, bank account numbers, Social Security Numbers, drivers' licence numbers, passport information, and various real estate transaction details[6]. Yahoo disclosed details of the 2013 breach as of December 2016, and subsequently had to revise the number of users affected from its initial calculus of 1 billion, to all 3 billion users, as reported in October 2017[7].

The second breach is "the 2014 breach [that] began with a 'spear phishing' email campaign sent to upper-level Yahoo employees. One or more of these employees fell for the bait, and Yahoo's data security was so lax, that this action was enough to hand over the proverbial keys to the kingdom," so allege the Plaintiffs[8]. In August 2016, a hacker posted for sale on the dark web the personal information of 200 million Yahoo users[9]. The Plaintiffs allege Yahoo was aware of the breach as of 2014 but did not publicly disclose this information until September 2016. In its September 2016 announcement, Yahoo stated that the affected "account information may have included names, email addresses, telephone numbers, dates of birth, hashed passwords, and, in some cases, encrypted or unencrypted security questions and answers[10]."

Finally, the Plaintiffs allege that Yahoo "quietly divulged" the existence of the "Forged Cookie Breach" in its quarterly US Securities and Exchange Commission filings as of 6 November 2016. The

continued

"Forged Cookie Breach" reportedly occurred sometime from 2015 to 2016 and allowed attackers to use forged cookies to access Yahoo users' accounts[11]. As cookies are text files placed on users' computers to store login information for the convenience of users, by forging these cookies the attackers were able to gain access and remain logged in to accounts for long periods of time.

Other related fallout

Separate and apart from the class litigation that followed, the breaches were the subject of a congressional inquiry as well as securities litigation. In her status as the former CEO of Yahoo, Marissa Mayer appeared before the US Senate Commerce Committee in November 2017 and testified that "Russian intelligence officers and state-sponsored hackers were responsible for" the attacks[12]. US prosecutors charged two Russian intelligence agents and two hackers in connection with one of the breaches[13].

Earlier in 2017, Yahoo shareholders filed a suit alleging federal securities fraud violations by failing to promptly disclose the breaches, which caused a subsequent stock price fall[14]. That case was assigned to the same judge who is handling the data breach class litigation (Judge Koh). Yahoo entered into a proposed settlement of that action in early March 2018, subject to court approval, agreeing to pay $80 million to settle those claims[15].

Class claims

The Plaintiffs filed suit in California and other federal courts, and the cases were consolidated in the United States District Court for the Northern District of California, San Jose Division[16]. The Plaintiffs alleged statutory violations of California consumer laws, like the Unfair Competition Law ('UCL') and the Data Breach Notification Law as well as the federal Stored Communications Act ('SCA').

The Plaintiffs asserted the causes of action were for breach of contract, breach of implied contracts, breach of the implied covenant of good faith and fair dealing, fraudulent inducement, negligence and negligent misrepresentation. In addition to declaratory relief and damages, the Plaintiffs sought punitive damages as a result of the alleged misrepresentations.

A variety of Plaintiffs

The First Amended Complaint ('FAC')[17] was filed by nine named Plaintiffs on behalf of four putative classes and one putative subclass. These included: Plaintiffs representing the US class and California sub-class; Yahoo account holders in Israel; small business users (who claimed Yahoo or Aabaco business accountholders in the US were compromised[18]); and, finally a class called 'Paid Users,' who include all paid Yahoo account holders in the US and Israel whose accounts were compromised[19].

Initial motion

In its initial motion to dismiss, Yahoo argued that the Plaintiffs lacked standing to file suit because they only alleged "vague and unspecified" harms. The Court held that the Plaintiffs had suffered sufficient injury by asserting "concrete and imminent threat of future harm" and loss of personally identifiable information[20] ('PII'). Yahoo did prevail on having the Stored Communications Act allegations dismissed as well as the California Online Privacy Act class claims, and non-resident Plaintiffs for Customer Records Act ('CRA') claims.

Surviving causes of action

In the second round of dismissal motions, Judge Koh again did not relieve Yahoo of all causes of action, letting stand Plaintiffs' claims for deceit by concealment, negligence, breach of contract, breach of implied contract, declaratory relief, and certain small business users' unfair competition and Consumers' Legal Remedies Act ('CLRA') claims. The Court began with a discussion of these small business users.

Small business users

The Court found that the named Plaintiff who asserted he "lost [a] benefit of the bargain" had standing to pursue his unfair competition claims because he alleged that the Defendants' "representations about security formed part of the reason for him to use Yahoo Mail in the first place and to pay $19.95 per year for the premium email service[21]." The Court found that "[s]uch benefit-of-the-bargain losses are sufficient to allege 'lost money or property,' and thus standing, under the UCL[22]." Later in its decision, the Court likewise found that the "remedies" claims by the small business user Plaintiff, Mortensen, were viable. Those allegations dealt with whether such a Plaintiff could allege that Yahoo Mail was a good or service, and Mortensen relied on Yahoo's representations regarding security. The Court found that Plaintiff Mortensen sufficiently alleged that only Yahoo could have known of the inadequacy of its security, and thus, he relied on its omissions regarding the service. The Court also found that Yahoo indeed provided a "service," under the relevant California Code provision[23].

Economic loss rule

Next the Court addressed the Defendants' arguments that deceit by concealment and negligence are barred according to the "economic loss rule" (which generally means that "purely economic losses [i.e., contractual obligations] are not recoverable in tort"). Here, the Court found that the Plaintiffs adequately pled a "special relationship" with the Defendants, when the Plaintiffs turned over PII with the understanding that the Defendants would protect it; that it was foreseeable that the Plaintiffs would suffer injury if their PII was not protected; that Defendants failed to promptly notify the Plaintiffs; and that the injury allegedly suffered was the result of the inadequate security. Thus, the Court found that the negligence claims should not be dismissed because the Plaintiffs sufficiently pled the necessary elements[24].

The Court also found that the Plaintiffs sufficiently identified the failure to warn of security problems, that they "plausibly" relied on the Defendants' actions and that they would have taken measures to protect themselves if they had been informed of security lapses. The Court also found that under California law, the Plaintiffs can seek recovery of compensatory damages, beyond out-of-pocket costs, for alleged deceit claims[25].

Yahoo argued that the Plaintiffs failed to allege that an officer, director or agent of the Defendants committed an oppressive, fraudulent, or malicious act, and that the specific causes of action do not warrant punitive damages.

Contract claims

The Court denied the Defendants' motion to dismiss the breach of contract claims. The Defendants argued that their terms of service barred recovery for damages other than direct damages. The Plaintiffs argued that these limitations are unconscionable. The Court found that the Plaintiffs made sufficient allegations to support procedural and substantive unconscionability, meaning that procedurally, a party had no opportunity to bargain for the terms, and, substantively, that the limitations were overly one-sided or harsh[26].

Punitive damages

Yahoo argued that the Plaintiffs failed to allege that an officer, director or agent of the Defendants committed an oppressive, fraudulent, or malicious act, and that the specific causes of action did not warrant punitive damages. The Court found that the Plaintiffs' had filed allegations against an officer or director by "focusing on particular conduct by the CISOs[27]." The Court also allowed the Plaintiffs to pursue punitive damages under the negligence claim, because the Plaintiffs alleged "numerous fraudulent, malicious, and oppressive acts [...] including that Defendants 'did nothing to protect its user data' and 'made a conscious and deliberate decision not to alert [its customers] [...][28]." The Court did however dismiss the punitive damages claim under the remedies claims and breach of good faith and fair dealing contractual claims.

A "trim" set of actions

Depending upon your point of view, indeed the Court did eliminate certain causes of actions and claims for punitive damages attendant to others[29]. However, the Court left standing some serious claims, including the allegations that the terms of service are potentially "unconscionable," that small business users did not get the "benefit-of-the-bargain," and that Yahoo executives were potentially deceitful. This same Judge, of course, presided over the *Anthem* class action, allowing claims under California's Unfair Competition Law and under New York's Deceptive Trade Practices Law[30]. While those motions were pending, the parties in *Anthem* proceeded to mediation, and not long after entry of the rulings the parties agreed to a $115 million settlement[31]. With this kind of judicial pressure on entities caught up in large data breaches, and in particular those that potentially had some delay in notification (perhaps even through no discernible fault), the stakes appear pretty high.

Indeed, the pre- and post-breach statements by chief executives will be intensely scrutinised, and likely quoted to bolster consumer claims of misrepresentation and the apparent lack of concern over or attention to customer's information. Obviously, the Yahoo scenario had immediate financial implications as well. Now that the securities piece of this problem has been resolved, one would expect the consumer litigation to follow the *Anthem* route toward settlement.

1. In Re: Yahoo! Inc. Customer Data Security Breach Litigation, No. 16-MD-02752-LHK; 'Order Granting in Part and Denying in Part Motion to Dismiss' Dkt. No. 205 (N.D. Calif., 9 March 2018). In 2017, Verizon, a telecommunications giant, completed its acquisition of Yahoo's core internet business. The acquisition was originally priced at $4.8 billion but as news of the breaches trickled out, Verizon sought a discount of $500 million and CEO Marissa Mayer announced her resignation. See https://www.usatoday.com/story/tech /news/2017/06/13/oath-arises-verizon-closes-deals-yahoo-former-ceo-mayer-departs/102793102/
2. Yahoo! Customer Data Security Breach at 2-3.
3. https://www.csoonline.com/article/2131970/identity-theft-prevention/yahoo-security-breach-shocks-experts.html
4. Yahoo! Customer Data Security Breach at 3.
5. Ibid. at p.4.
6. Ibid.
7. https://www.wired.com/story/yahoo-breach-three-billion-accounts/, 'Yahoo [in December 2016] announced that private data from more than a billion user accounts was stolen in 2013 by an unspecified hacker.' https://www.mercurynews.com/2016/12/15/yahoos-failures-led-to-billion-account-breach-experts-say/; The breach was believed to be the largest reported data breach ever. See https://www.usatoday.com/story/tech/2017/10/03/3-billion-yahoo-users-breached-company-says/729155001/
8. Yahoo! Customer Data Security Breach at 5.
9. Ibid.
10. Ibid. at p.6.
11. Ibid.
12. https://www.reuters.com/article/us-usa-databreaches/former-yahoo-ceo-apologizes-for-data-breaches-blames-russians-idUSKBN1D825V
13. http://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html
14. In Re: Yahoo! Inc. Securities Litigation, No. 5:17-00373 (LHK) (N.D. Cal.).
15. https://www.dandodiary.com/2018/03/articles/securities-litigation/yahoo-settles-data-breach-related-securities-suit-80-million/
16. https://www.lexislegalnews.com/articles/17606/yahoo-moves-to-dismiss-data-breach-class-action-for-lack-of-standing
17. See infra; following the initial dismissal motion, Plaintiffs filed an amended complaint.
18. https://www.ecommercebytes.com/2017/09/04/yahoo-stores-gets-name-back-dizzying-ride/
19. Yahoo! Customer Data Security Breach Litigation, No. 16-MD-02752-LHK, at p.7-9. The US class consists of all 'free' account holders, i.e., those who did not pay a fee for email accounts.
20. In Re: Yahoo! Customer Data Security Breach Litigation, 'Order Granting in Part and Denying in Part Motion to Dismiss,' Dkt. No. 94 (N.D. Calif., 30 August 2017).
21. Yahoo! Customer Data Security Breach at 17.
22. Ibid. Citing one of her own prior rulings in another breach case: In re Anthem, Inc. Data Breach Litig., No. 15-MD-02617-LHK, 2016 WL 3029783, at *30 (N.D. Cal. May 27, 2016).
23. Yahoo! Customer Data Security Breach at 34.
24. Ibid. at p.20.
25. Ibid. at p.24.
26. Ibid. at p.25-28.
27. Ibid. at p.43.
28. Ibid. at p.45.
29. https://www.mercurynews.com/2018/03/13/yahoo-loses-bid-to-dismiss-data-breach-lawsuit/; see also https://www.bna.com/yahoo-dodges-class-n73014464006/
30. In Re: Anthem, Inc. Data Breach, supra.
31. https://www.bloomberg.com/news/articles/2017-06-23/anthem-reaches-115-mln-settlement-in-massive-data-breach-case