



## ***KD Alert: Does Holland v. Yahoo! Prove That The Ninth Circuit Will Remain The Post-Clapper Outlier?***

By Hsiao (Mark) C. Mao, Esq. and Sheila Pham, Esq.

*The Ninth Circuit is often likened to the legal “Wild-Wild-West.” For data breach litigation, things are apparently no different.*

*For the last two years, it appeared as if data breach litigation would be defeated by the Supreme Court’s decision in Clapper v. Amnesty Intern. USA. In Clapper, which started out as a wiretap case, the Supreme Court held that plaintiffs must show “certainly impending injuries in fact” to establish Article III standing. 133 S.Ct. 1138 (2013).*

*Thereafter, almost all of the courts faced with data breach claims followed the Supreme Court’s test, requiring injuries to be “certainly impending.” Given the difficulties of showing actual damages and causation following loss of personally identifiable information (PII), few plaintiffs have passed the test:*

- *Green v. EBay Inc.*, Case No. 14-cv-01688-SM-KWR (E.D. La. May 4, 2015) [no standing in case involving cyber attack exposing user passwords, names, and other PII];
- *Storm v. Paytime, Inc.*, Case No. 14-cv-01138 (M.D. Pa. Mar. 13, 2015) [no standing in case involving hacking of national payroll firm];
- *Peters v. St. Joseph Serv. Corp.*, Case No. 14-cv-2872 (S.D. Tex. Feb. 11, 2015) [no standing in case involving infiltration of network of health care provider storing personally identifiable health information];
- *Lewert v. P.F. Chang’s China Bistro*, Case No. 2014-cv-04787 (N.D. Ill. Dec. 10, 2014) [no standing in case where plaintiffs claimed that restaurant chain failed to secure their credit card information];
- *Remijas v. The Neiman Marcus Group, LLC*, Case No. 14-cv-01735 (N.D. Ill. Sept. 16, 2014) [no standing in case involving unauthorized access to customers’ credit card information];
- *Burton v. MAPCO Express Inc.*, Case No. 2013-cv-00919 (N.D. Ala. Sept. 12, 2014) [no standing in case involving unauthorized access of customer’s account information];
- *In re Science Applications International Corp. Backup Tape Data Theft Litig.*, MDL Case No. 2360 (D.C. May 19, 2014) [no standing in case involving theft of data tapes with information concerning U.S. military and their families];
- *Strautins v. Trustwave Holdings Inc.*, Case No. 12-09115 (N.D. Ill. Mar. 12, 2014) [no standing in case alleging data company’s malfeasance led to breach of South Carolina’s Department of Revenue];
- *Galeria v. Nationwide Mut. Ins. Co.*, 998 F. Supp. 2d 646 (S.D. Ohio 2014) [no standing in case involving authorized access to plaintiffs’ information provided to insurance company];
- *Polanco v. Omnicell Inc.*, 13-1417 (NLH/KMW) (D.N.J. Dec. 26, 2013) [no standing in case involving theft of an employee laptop containing unencrypted information];
- *In re Barnes & Noble Pin Pad Litig.*, 12-cv-8617 (N.D. Ill. Sept. 3, 2013) [no standing in case involving tampering with personal identification number pads used to process payment information].

*However, a minority number of courts – notably a few in the Ninth Circuit – have taken considerable effort to avoid applying the Supreme Court’s standard for standing in Clapper. See In re Sony Gaming Networks & Customer Data Sec. Breach Litig., MDL No. 11MD2258 AJB (MDD) (S.D. Cal. Jan. 21, 2014) [finding a “credible threat of impending harm”]; see In re Adobe Systems Inc. Privacy Litig., 13-05226 (N.D. Cal. Sept. 4, 2014) [finding an “immediate and very real” risk of harm]. Although such decisions are by far the minority, their existence does not bode well for deterring future cyber breach class actions. See also In re Target Corp. Customer Data Security Breach Litig., MDL No. 14-2522 (D. Minn. Dec. 18, 2014) [finding that Target had set “a too-high standard for Plaintiffs to meet at the motion-to-dismiss stage.”]*

*Indeed, Northern California District Court Judge Lucy H. Koh, who wrote the opinion in Adobe Systems, seems bent on solidifying a different test for Article III standing in the Ninth Circuit. Recently on May 26, Judge Koh granted class action certification in an alleged*

wiretapping case again using the “immediate and real” test. *Holland v. Yahoo! Inc.*, 13-cv-04980 (N.D. Cal. May 26, 2015). Plaintiffs who were not subscribers of Yahoo! claimed that the company intercepted and mined data from their email messages for the purposes of targeted advertising. Yahoo! retained copies of e-mails to and from its subscribers, thereby also intercepting the communications of non-subscribers.

In discussing standing, Judge Koh repeated that the allegations of the email users suggested a “real and immediate threat” for future harm, which was the same test she applied in *Adobe Systems*. As if she was writing for progeny, Judge Koh emphasized her point citing other cases discussing “real and immediate threat(s)” and similar language, without citing to any cases using a “certainly impending” standard. (See *id.*, May 26, 2015 order, at p. 11.) Comparing the two tests, showing a “real and immediate threat” requires less.

Ironically, recent reports indicate that data breach cases filed in the Ninth Circuit have actually been on the decrease.