The Coming Wave of California Consumer Privacy Act Lawsuits

February 17, 2020 – The TMCA
by Kent J. Schmidt and Robert E. Cattanach

Since the beginning of the year, industry leaders and counsel advising clients on data security issues have held their collective breath in anticipation of the tsunami of California Consumer Privacy Act (CCPA) lawsuits. The CPPA, ballyhooed over the past few years as the next big thing in consumer litigation, is now the law in California. The most comprehensive cybersecurity and information privacy statutory scheme in the nation, the CCPA creates an express private right of action for individuals whose data is breached by hackers and mandates that significant penalties be assessed against the company that violates cybersecurity standards.

While no CCPA lawsuits were filed in January, a consumer privacy lawsuit filed February 3 in the U.S. District Court for the Northern District of California has garnered a great deal of attention. Touted by some as the "first" CCPA case, a closer reading of the Complaint filed in Barnes v. Hanna Anderson, LLC (No. 3:20-CV-00812) shows that the plaintiff does not assert a direct claim under the statute. There is a simple reason for this. The data breach alleged in Barnes occurred in 2019, before the effective date of the CCPA. Although the Complaint alleges acts or omissions in 2020 by stating that the retailer did not tell customers or the Attorneys General about this in January, the fact that the data breach occurred before the effective date of the CCPA would render a direct claim subject to a motion to dismiss.

As the industry pivots from the compliance questions that dominated the pre-effective

Related People

- Kent J. Schmidt

Related Capabilities

- Trademark, Copyright + Advertising
- Intellectual Property Litigation

period and begins to focus on CPPA litigation, this lawsuit gives us a few insights into future CCPA claims coming to a California courthouse near you:

1. **The Reasonable Security Measures Standard**. The Barnes Complaint illustrates the framing of the core issue in a CCPA data breach claim: whether the company utilized "reasonable security measures" under the statute—whatever that may mean. Recognizing that swiftly evolving technology in this area makes it unworkable to incorporate specific technical requirements in the statutory standard (although previous guidance by California's then-Attorney General Kamala Harris gives us some clues), the California Legislature has opted for a qualitative standard. The statutory predicate for a civil cause of action illustrates this: "Any consumer whose nonencrypted and nonredacted personal information . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the **duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information** may institute a civil action." Cal. Civ. Code § 1798.150(a)(1) (emphasis added). Although this standard has the benefit of being adaptable to changing technology, it perpetuates a "hindsight" problem often encountered in data breach litigation: it is exceedingly easy for a plaintiff, with the benefit of hindsight, to persuasively argue that some further act would have been reasonable at the time and that the breach was foreseeable. The Complaint filed in Barnes contends that this standard was not met in a variety of ways and cites to another provision of the law which requires companies to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." Cal. Civ. Code § 1798.81.5(b). Whether it will be inadmissible as a subsequent remedial measure, the Complaint even cites to a LinkedIn posting after the alleged data breach in which Hanna Andersson announced it was searching for a new "Director of Cyber Security," suggesting that this position was not filled when the data was hacked. (Compl. ¶ 33.) The Complaint further alleges that the reasonable measures standard is informed by not only the CCPA but the Federal Trade Commission Act ("FTC Act") (15 U.S.C. § 45(a)) and various other standards and FTC publications. (Compl. ¶ 33.) These are all paths to one destination—the core litigated issue in this case and every other CCPA lawsuit that will be filed—whether the plaintiff will be allowed to use hindsight to prove that the defendant breached these evolving standards of care in cybersecurity.
2. **Interplay Between CCPA and other Statutory and Common Law Remedies.** In lieu of a direct claim for violation of the CCPA, the Barnes Complaint alleges a common law claim for negligence as well as a claim for violation of the California's Unfair Competition Law ("UCL") (Cal. Bus. & Prof. Code § 17200). The negligence claim is presumably included to provide a basis for claims by non-California residents based on the theory that defendants breached a duty of care to those class members. The inclusion of the UCL claim is a staple of any California consumer class action. That statute provides remedies for any business practice that is proven to be unfair, fraudulent or unlawful. It will be interesting to see how the courts address the interplay between the UCL and the CCPA since the latter provides that "[n]othing in this title shall be interpreted to serve as the basis for a private right of action under any other law." Cal. Civ. Code § 1798.150(c). In response to future CCPA claims, defense counsel may argue that a direct claim under the CCPA is the exclusive remedy and a separate UCL claim predicated solely on the CCPA is not actionable by the plain language of the statute.
3. **Contribution and Indemnity Issues in Secondary Litigation**. This lawsuit names both the retailer (Hanna Andersson, LLC) and the ecommerce vendor (Salesforce.com, Inc.) that supplied the platform. The inclusion of both defendants is a reminder that, like other consumer protection lawsuits, these claims may trigger a

secondary category of cross-claims between businesses and their ecommerce and cybersecurity vendors, including claims for contribution and indemnity. This will often be the case regardless of whether the secondary party is also named directly by the consumer (as Salesforce was here). It advisable to review provisions in contract documents with third party vendors—including caps and limitations on damages—as such contract language will be paramount in secondary claims. These second-tier claims are in addition to insurance coverage questions and lawsuits that these cases will likely spawn.

4. **The Learning Curve for Courts.** Even a cursory reading of the Complaint serves as a reminder that CCPA cases bring inherent challenges for litigants on both sides stemming from the fact that most individuals are unfamiliar with all but the most rudimentary aspects of cybersecurity. In theory, a trier of fact may have to address the reasonableness of the defendant's cybersecurity measures and get 'deep into the weeds' of these technical issues. But as noted earlier, as a practical matter, juries, and perhaps even some judges, will be attracted to the hindsight argument of "how did the defendant not protect against this obvious vulnerability?" Effectively litigating these cases will require trial counsel experienced not only with an understanding of the technical aspects of cybersecurity and the requirements of the statutes and regulation, but also savvy enough to appreciate and dismantle the attractive "hindsight" arguments plaintiffs' counsel are sure to appeal to, if not expressly espouse.

The fact that there has only been one quasi-CCPA lawsuit in the first several weeks of 2020 is not an indication that the predictions of tidal wave of CCPA class actions were overblown. As the Barnes filing illustrates, there are thorny questions concerning the retroactive application of the CCPA to data breaches that occurred before January 1. It is likely that there will be a lag of a few months as plaintiff lawyers wait to find cleaner cases in which the data breach occurred after the effective date. As this and other lawsuits make their way through motion practice, trials and appeals, there will be greater clarity to these and other questions in this emerging sector of class action litigation.