LOS ANGELES & SAN FRANCISCO
Daily Journal
www.dailyjournal.com

THURSDAY, MAY 21, 2020

PERSPECTIVE

Can companies be liable if third-party contractors suffer data breaches?

By Peter S. Selvin

The California Consumer Privacy Act became effective on Jan. 1. Included among its provisions is the grant of a private right of action on behalf of 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." Civil Code Section 1798.150.

An interesting question is whether a company may face liability under this statute (or based on common law theories) where one of its vendors or third-party contractors to whom it has entrusted the personal information of its customers or clients suffers a data breach. The possibility for liability in such a scenario was addressed in a recent case from Delaware.

In *Eugenia v. Laboratory Corporation of America Holdings*, C.A. No. 2020-0305-PAF, filed in Delaware's Chancery Court on April 28, plaintiffs asserted derivative claims action against LabCorp's directors and officers arising from a data breach suffered by American Medical Collection Agency (AMCA), a third-party vendor whom LabCorp had engaged to collect patient receivables for medical labs. Plaintiffs alleged that as a result of the breach, 10.2 million LabCorp patients had their personal information compromised. Plaintiffs alleged that company's officers and directors had breached their fiduciary duties by, among other things, providing patients' personal and health information to a third-party contractor that failed to use adequate cybersecurity safeguards.

Plaintiffs' liability claims in that case were buttressed by the fact that AMCA was allegedly a "business associate" of LabCorp under the Health Insurance Portability and Accountability Act. As such, LabCorp had an obligation to ensure that AMCA had appropriate safeguards in place to protect the privacy of the information. But even apart from the particular obligations arising under HIPPA, this case raises the question of whether under the CCPA companies may be subject to liability if their vendors or third-party contractors to whom they have entrusted confidential information suffer a data breach. In broad terms, the plaintiffs in *Eugenia* alleged that where a company entrusts private data to others, the company has an obligation to scrutinize and monitor the cybersecurity practices of their contractors and vendors with whom they do business.

In this regard, it may important for insurance coverage purposes under a CGL policy whether a data breach has been suffered by the insured company itself or a contractor or vendor of the insured. This is because of the "publication" requirement in the "personal and advertising injury" coverage that is afforded under most CGL policies.

In this regard, most CGL policies offer coverage for "personal and advertising injury," which is often referred to as Coverage B. This form of coverage is triggered by certain enumerated offenses typically including "injury arising out of oral or written *publication*, in any manner, of material that violates a person's right of privacy."(Emphasis added). As the dissemination of one's personal information without consent violates a person's right of privacy, several cases have addressed whether liability claims arising data breaches may be covered under a CGL policy's "personal and advertising injury" coverage.

A key issue in these coverage cases has been whether the requirement of a "publication" has been met. In this regard, the majority view seems to be that a covered "publication" within the meaning of Coverage B must have been made *by the insured*, not by a third party, such as a negligent vendor or third-party contractor. Thus, the cases fall into two categories: those where the insured directly made the "publication" of personal data and those where the "publication" was made by a third party.

In *Travelers Indemnity Company v. Portal Healthcare Solutions*, 35 F.Supp. 3d 765 (E.D.Va. 2014), aff'd, 644 Fed. Appx. 245 (4th Cir. 2016), is an example of the first category of cases. In that case, Portal Healthcare Solutions, a business specializing in the electronic safekeeping of medical records for hospitals, clinics and other medical providers, was sued in a class action by two patients of a hospital (Glen Fall) for which Portal provided electronic record-keeping services.

The class action arose because certain confidential patient records appeared on the internet, causing those records to become publicly accessible. The class action complaint alleged that patients' confidential records were accessible and downloadable from the internet by unauthorized persons without security restrictions by a more than one-year period.

The class complaint alleged that "Portal posted confidential individual records on the internet, making the records available to anyone who searched a patient's name and clicked on the first result." In other words, the data leak allegedly resulted from conduct by the insured, not by a third party.

In these circumstances, the court found coverage for the class claims. In this regard, the core issue in the coverage dispute was whether exposing material to online searching of a patient's name constituted "publication" of electronic materials within the meaning of the policy. The district court answered this question in the affirmative, rejecting Travelers' primary argument that because the data leakage was supposedly unintentional on Portal's part, there could be no "publication." The district court rejected this argument, holding that "the issue cannot be whether Portal intentionally exposed the records to public viewing since the definition of 'publication' does not hinge on the would-be publisher's intent. Rather, it hinges on whether the information was placed before the public." The 4th Circuit affirmed this result.

See also Evanston Ins. Co. v. Gene by Gene, Ltd., 155 F.Supp.3d 706, 708 (S.D. Tex. 2016) (coverage found where insured published DNA results on its website without the individual's consent).

By contrast, where the "publication" has been made by a third party — as in the *Eugenia* case — the courts have taken a different approach. Thus, in *Zurich Am. Ins. Co. v. Sony Corp.*, 2014 WL 3253541 (N.Y. Sup. Ct. February 24, 2011), a computer hacker broke into Sony's computer system and then posted the certain private and personal information on the internet. Determining that a covered "publication" must have been made by the insured — and not by a third party — the court found no coverage for the incident. The court in *Innovak International v. Hanover Insurance Company*, 280 F.Supp. 3d 1340 (M. D. Fla. 2017), reached a similar outcome as did the court in *St. Paul Fire & Marine Insurance Company v. Rosen Millennium, Inc.*, 6:17-cv- 540 (M.D. Fla. 2018) (finding that third-party data breaches are not covered under CGL policies).

Finally, it should be noted that coverage under a CGL policy should be the last resort for an insured hit with a data breach claim, regardless of whether it originates with the insured itself or a third party. This is primarily because of the "Access or Disclosure of Confidential or Personal Information and Data-Related Liability Exclusion" which was introduced in 2014 and which may preclude coverage for these kind of events. The existence of this exclusion highlights the need for specialized cyber-insurance for companies that receive or process personal or private information. ■

Peter S. Selvin *is a partner at Ervin Cohen & Jessup LLP. You can reach him at pselvin@ecjlaw.com.*