DREHER TOMKIES LLP ALERT

FOR CLIENTS AND FRIENDS OF DREHER TOMKIES LLP

April 27, 2020

ROUND-UP OF THE FIRST WAVE OF CCPA CLASS ACTION LAWSUITS

The California Consumer Privacy Act ("CCPA") went into effect on January 1, 2020. *See* our prior ALERTS dated July 18, 2018 and September 19, 2019 for a brief summary of the CCPA and enacted amendments. Although the final regulations that are to accompany the CCPA have not been finalized, the California Attorney General may begin enforcement of the CCPA on July 1, 2020. *See* our prior ALERT dated March 13, 2020.

In addition to the Attorney General's enforcement power, the CCPA gives California residents a limited private right of action to recover damages if 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. A handful of plaintiffs have seized the opportunity to exercise this right by bringing class action lawsuits against a wide range of companies.

***Barnes v. Hanna Anderson, LLC and Salesforce.com, Inc.*, No. 4:20-cv-00812 (N.D. Cal. Feb. 3, 2020)**

A California resident filed a class action lawsuit against a retail company and its third party ecommerce platform (collectively "retail company") after the retail company experienced a data breach from September 16, 2019, to November 11, 2019, that resulted in hackers accessing customer payment card numbers, CVV codes and credit card expiration dates and selling this information on the dark web. The complaint establishes a nationwide class and a separate "California class" that includes all persons residing in California whose personal identifiable information was compromised in the data breach.

The complaint sets forth four causes of action but does not cite a cause of action under the CCPA. Instead, the complaint declares that the plaintiff and California class members reserve the right to amend the complaint as of right to seek damages and relief under the CCPA. The complaint also states that the class members have questions of law and fact in common, including whether the retail company violated the CCPA by failing to maintain reasonable security procedures and practices appropriate to the nature of the personal identifiable information.

***Sheth v. Ring, LLC*, No. 2:20-cv-01538 (C.D. Cal. Feb. 18, 2020)**

A Washington resident filed a class action lawsuit against a security and smart home company for sharing its customers' personal information in real time with unauthorized third parties without the customers' informed consent. The complaint alleges that the security company fails to implement common and basic cybersecurity measures or protocols to guard against unauthorized access or intrusion by third parties, including not requiring customers to use two-factor authentication to access security devices or accounts. The complaint also alleges that the security company's smartphone app has third-party trackers sending out a plethora of customers' personally identifiable information with four analytics and marketing companies.

Among the eight causes of action set forth in the complaint, the plaintiff alleges that the security company violated the CCPA by collecting and using personal information without providing consumers with notice consistent with the CCPA, and failing to provide notice to consumers of their right to opt-out of the company's sale of their personal information to third parties.

***Fuentes v. Sunshine Behavioral Health Group LLC*, No. 8:20-cv-00487 (C.D. Cal. Mar. 10, 2020)**

A Pennsylvania resident filed a class action lawsuit against a drug and rehabilitation facility for a data breach that occurred in September 2019 which resulted in exposure of sensitive personal and medical information of approximately 3,500 patients. The rehabilitation facility has facilities in California, Colorado and Texas. The named plaintiff was a patient from January 2019 to February 2019.

The complaint alleges that the data breach began in March 2017 but the rehabilitation center did not learn of the breach until September 2019. The complaint alleges that the rehabilitation center filed a notice of data breach with state attorney general and sent a notification to affected consumers on January 21, 2020. Among the 12 causes of action set forth in the complaint, the plaintiff alleges that the rehabilitation facility violated the CCPA by subjecting nonencrypted and nonredacted personal and medical information to unauthorized access and exfiltration, theft or disclosure as a result of the rehabilitation facility's violation of its duty to implement and maintain reasonable security procedures and practices appropriate to

Darrell L. Dreher
ddreher@dltlaw.com

Elizabeth L. Anstaett
eanstaett@dltlaw.com

Emily C. Cellier
ecellier@dltlaw.com

Susan L. Ostrander
sostrander@dltlaw.com

2750 HUNTINGTON CENTER
41 S. HIGH STREET
COLUMBUS, OHIO 43215
TELEPHONE: (614) 628-8000 FACSIMILE: (614) 628-1600
WWW.DLTLAW.COM

Michael C. Tomkies
mtomkies@dltlaw.com

Susan M. Seaman
sseaman@dltlaw.com

Lindsay P. Valentine
lvalentine@dltlaw.com

Judith M. Scheiderer
jscheiderer@dltlaw.com

Robin R. De Leo
robin@deher-la.com

the nature and protection of that information. The complaint states that the consumer's counsel served the rehabilitation center with notice of the CCPA violations by certified mail, as required by the statute.

***Almedia v. Slickwraps Inc.,* No. 2:20-at-00256 (E.D. Cal. Mar. 12, 2020)**

Three California residents filed a class action complaint against a company that makes and sells an assortment of cases for mobile phones, tablets and other electronic devices for a data breach that the company suffered in February 2020 which resulted in exposure of personal identifiable information of at least 858,000 customers. The complaint alleges that the company was informed of security vulnerabilities of its website by a third party cybersecurity analysis but that the company did nothing to fix the inadequacies or prevent a future data breach.

The complaint sets forth six causes of action, including an action for deprivation of rights possessed under the California Unfair Competition Law ("CA-UCL") and CCPA. The complaint alleges that the plaintiffs and class members were injured in that they were deprived of rights they possess under the CA-UCL and CCPA to keep their personal identifiable information secure and confidential.

***Cullen v. Zoom Video Communications, Inc.*, No. 5:20-cv-02155-SVK (N.D. Cal. Mar. 30, 2020)**

A California resident filed a class action lawsuit against the online video conferencing platform for failing to properly safeguard the personal information of the millions of users that use the platform and collecting and sharing this personal information with third parties. The complaint alleges that the video conferencing app notifies Facebook when the user opens the app, of details on the user's device such as the model, the time zone and city they are connecting from, which phone carrier they are using and a unique advertiser identifier created by the user's device that companies can use to target a user with advertisements. The complaint alleges that the video conferencing platform failed to implement adequate security measures and permitted unauthorized third-party tracking of consumers' personal information.

The complaint sets forth six causes of action, the first being a violation of the CCPA. The complaint alleges that the video conferencing platform violated the CCPA by collecting and using personal information without providing consumers with adequate notice consistent with the CCPA. The complaint also alleges that the video conferencing platform further violated the CCPA by failing to prevent the plaintiff's and the class members' nonencrypted and nonredacted personal information from unauthorized disclosure as a result of the platform's violation of its duty to implement and maintain reasonable security procedures and practices.

Although these class action lawsuits allege valid data security practice violations, most of the lawsuits should not survive motions to dismiss for a variety of reasons. First, the CCPA only protects and applies to California residents. The only named plaintiffs in two of these cases are not California residents and would not have standing to bring an action under the CCPA.

Second, as noted above, the CCPA only gives a California resident a right of action if the consumer's nonencrypted and nonredacted personal identifiable 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. A consumer does not have the power under the CCPA to bring an action against a business for failing to provide adequate disclosures and notice, as alleged in the *Zoom* complaint.

We will continue to actively monitor and report on other CCPA updates. The full text of the CCPA can be found in our Firm's Marketing and Privacy Digest. We can assist businesses in complying with the privacy policy and notice requirements of the CCPA. Please let us know if you have any questions. ❑

✧ *Mike Tomkies and Lindsay Valentine.*