STINSON

News & Insights

Healthtech and FinTech Security a Focus of Recent CCPA Litigation and Enforcement

Alert

09.22.2020

By Steve Cosentino, CIPP and Jeffrey Kettle, CIPP

As anticipated by many experts in the field, the data security-focused private right of action under the California Consumer Privacy Act (CCPA) has resulted in claims alleging potential unauthorized access. FinTech data aggregator Yodlee finds itself defending a class-action complaint in the Northern District of California concerning their alleged failure to protect personal information by sharing data in unencrypted format. Yodlee allegedly collected data from software products provided to many banks, financial institutions and other FinTech companies, and marketed and sold such data to large financial institutions without proper disclosures or data protection.

Regulators are also focusing on security in enforcement actions. On September 17, Attorney General Xavier Becerra announced a major settlement against healthtech company Glow, Inc., requiring Glow to pay a $250,000 fine and comply with state consumer protection and privacy laws applicable to a fertility tracking app. The complaint alleged that Glow failed to adequately safeguard health information, allowed access to personal information without consent and failed to address app security problems that could have allowed third parties to reset user passwords and access personal information without consent.

FINAL CCPA REGULATIONS

In the meantime, last month, the final text of the CCPA regulations was approved and filed with the California Secretary of State. As described by Attorney General Xavier Becerra, the "rules guide consumers and businesses alike on how to implement the California Consumer Privacy Act." Noteworthy was the filing of an addendum on July 29 by the Office of the California Attorney General, making changes to the rulemaking package submitted in June. While the majority of the revisions are non-substantive in nature, one reversal in particular is noteworthy, providing further insight into notice requirements under the

CCPA.

As stated in the "Amended Notice of Approval in Part and Withdrawal in Part of Regulatory Action," several sections were withdrawn, including section 999.305(a)(5). The rationale behind the removal of section 999.305(a)(5) is perhaps the most unclear, and likely has the most practical effect on a business. Regarding a business's "Notice at Collection of Personal Information," this section had required that a business attain "explicit consent from the consumer" when it planned to use "consumer's personal information for a purpose materially different than those disclosed in the notice at collection." The regulations now only require that the "business shall provide a new notice at collection." This is a dramatic reverse-course. In the "Final Statement of Reasons," the importance of this now-deleted requirement was described as follows: "Just as a business must provide a notice at or before the point of collection so that the consumer may affirmatively decide whether to proceed with the interaction, subsection (a)(5) is necessary so that the consumer may affirmatively decide whether to agree to the new use."

ON THE HORIZON

With the regulations finalized, the California Legislature took steps to reduce another significant contingency in the CCPA, passing AB-1281 to extend the B2B and HR exemptions to the CCPA for another year to January 1, 2022. That bill is awaiting approval by California Governor Gavin Newsom.

In November, the state's general election will include the California Privacy Rights Act (CPRA) ballot initiative that would expand the privacy restrictions included in the CCPA. The CPRA would extend the B2B and HR exemptions to January 1, 2023 when the CPRA would take effect. The CPRA includes new limitations on the use of sensitive personal information such as government identifiers, account and loan information, precise geolocation, racial or ethnic origin, religious or philosophical beliefs, union membership, contents of mail, email and text messages, genetic data and certain sexual orientation, health and biometric information. The CPRA would provide some business-friendly changes such as a limit on liability for violations of the law by third-party businesses and a significant exception to deletion and access rights for many types of unstructured data. There is also a potential exemption to the broad definition of sale relating to sharing personal information for some cross-context behavioral advertising. It would clarify that companies can offer loyalty and rewards programs and exempt more small businesses.

NEXT STEPS FOR YOUR BUSINESS

The Yodlee and Glow matters emphasize the need for encryption wherever possible along with other security measures such as two-factor authentication. Companies should ensure that they have a well-developed written information security program in place. Keep an eye out for the signing of AB-1281 as well as the potential passage of the CPRA. Both will necessitate privacy policy and compliance document changes relating to the duration of the B2B and HR exemptions.

Healthtech and FinTech Security a Focus of Recent CCPA Litigation and Enforcement

CONTACT

Stephen J. Cosentino, CIPP

RELATED CAPABILITIES

Banking & Financial Services

Cybersecurity & Data Privacy

Health Care & Life Sciences

Intellectual Property & Technology