



July 18, 2018

## CALIFORNIA ENACTS THE CALIFORNIA CONSUMER PRIVACY ACT OF 2018

On June 28, 2018, the California governor signed California A.B. No. 375 that enacts the California Consumer Privacy Act of 2018 ("Act"), effective January 1, 2020. Financial institutions already are subject to notice and opt-out requirements under the federal Gramm-Leach-Bliley Act privacy provisions ("GLBA") and the California Financial Information Privacy Act. The new California Act applies more broadly than GLBA and grants consumers a right to request a business to disclose (i) the categories and specific pieces of personal information that it collects about the consumer, (ii) the categories of sources from which that information is collected, (iii) the business purposes for collecting or selling the information and (iv) the categories of third parties with which the information is shared. Under the Act, a business must make available to consumers two or more designated methods for submitting requests for information requests. The Act does not apply to: (i) the sale of personal information to or from a consumer reporting agency if that information is to be reported in, or used to generate, a consumer report as defined by 15 U.S.C. § 1681a(d) and use of that information is limited by the federal Fair Credit Reporting Act; and (ii) personal information collected, processed, sold or disclosed pursuant to the Gramm-Leach-Bliley Act of 1999, if it is in conflict with that law. Thus, financial institutions subject to GLBA may be less impacted than other business entities.

A requirement in the Act not found in GLBA gives a consumer the right to request that a business delete any personal information about the consumer which the business has collected from the consumer in certain situations. The Act contains multiple disclosure requirements a business that collects or sells consumers' personal information must provide to consumers, including:

- (1) A notice informing consumers as to the categories of personal information to be collected and the purpose for which the categories of personal information may be used, at or before the point of collection;
- (2) The consumer's right to request the deletion of the consumer's personal information;
- (3) The category or categories of consumers' personal information it has sold, and the category or categories of

consumers' personal information is has disclosed for a business purpose; and

- (4) Notice that consumers' personal information may be sold and that consumers have the right to opt-out of the sale of their personal information.

These are similar to what financial institutions are required to provide with the addition of the right to request deletion of information.

The scope of the Act is illustrated by the definitions, including the definition of "personal information," which means information that identifies, relates to, describes, is capable of being associated with or could reasonably be linked, directly or indirectly, with a particular consumer or household. "Personal information" includes, but is not limited to, the following: (i) identifiers such as a real name, alias, postal address, unique personal identifier, online identifier Internet Protocol address, email address, account name, social security number, driver's license number, passport number or other similar identifiers; (ii) any categories of personal information described in Section 1798.80(e) (regarding customer records); (iii) characteristics of protected classifications under California or federal law; (iv) commercial information, including records of personal property, products or services purchased, obtained, or considered or other purchasing or consuming histories or tendencies; (v) biometric information; (vi) internet or other electronic network activity information, including, but not limited to, browsing history, search history and information regarding a consumer's interaction with an Internet Web site, application or advertisement; (vii) geolocation data; (viii) audio, electronic, visual, thermal, olfactory, or similar information; (ix) professional or employment-related information; (x) education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. section 1232g, 34 C.F.R. Part 99); and (xi) inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities and aptitudes.

Unlike the GLBA, the Act provides consumers with a private right of action in the event any consumer whose nonencrypted or nonredacted personal information is subject to an unauthorized

Darrell L. Dreher  
ddreher@dtlaw.com

Elizabeth L. Anstaett  
eanstaett@dtlaw.com

Emily C. Cellier  
ecellier@dtlaw.com

Susan L. Ostrander  
sostrander@dtlaw.com

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

To see previously sent ALERTS, visit our website at [www.dtlaw.com](http://www.dtlaw.com)

To decline future ALERTS, please contact us at [ALERTS@DLT.LAW.COM](mailto:ALERTS@DLT.LAW.COM). This ALERT has been prepared for informational purposes only. It does not constitute legal advice and does not create an attorney-client relationship.

Michael C. Tomkies  
mtomkies@dtlaw.com

Susan M. Seaman  
sseaman@dtlaw.com

Lindsay P. Valentine  
lvalentine@dtlaw.com

Judith M. Scheiderer  
jscheiderer@dtlaw.com

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



access, theft or disclosure as a result of the business' violation of the duty to implement and maintain reasonably security procedures and practices. Prior to initiating an individual or class action, a consumer must provide 30 days' notice to the business to cure the violation.

This Act comes at a time when businesses are adjusting their privacy and information practices to comply with the EU General Data Protection Regulation ("GDPR"). The GDPR requires businesses that handle European customers' personal information to disclose how they use customers' personal information and provide customers with a way to opt-out of sharing their personal information.

Financial service providers will need to analyze the new law to determine how the law works with GLBA and the expanded requirements. The full text of the Act will be added to our firm's Marketing and Privacy Digest. Please contact us with questions or for assistance in preparing for compliance by January 1, 2020. ☐

✧ *Elizabeth Anstaett and Lindsay Valentine*

**LOOKING FOR A MARKETING AND PRIVACY COMPLIANCE**

**RESOURCE?** We publish an easy-to-use reference, our **MARKETING AND PRIVACY DIGEST**, that compiles the state laws governing financial privacy, fair credit reporting, telemarketing/automatic dialing and announcing devices, telephone monitoring and recording, electronic signatures and restrictions on the use of social security numbers by financial service providers. Creditors, marketers and servicers should find this resource invaluable to marketing and privacy program development and regulatory compliance. **Contact us for details.**