BakerHostetler

Baker&Hostetler LLP

11601 Wilshire Boulevard
Suite 1400
Los Angeles, CA 90025-0509

T 310.820.8800
F 310.820.8859
www.bakerlaw.com

Alan L. Friel
direct dial: 310.442.8860
afriel@bakerlaw.com

March 8, 2019

Via U.S. Mail and Email:
PrivacyRegulations@doj.ca.gov

CA Department of Justice
Attn: Privacy Regulations Coordinator
300 S. Spring Street
Los Angeles, CA 90013

Re: CCPA Regulations

To Whom It May Concern:

BakerHostetler LLP has one of the nation's leading privacy and data security legal practices as recognized by numerous rankings and awards, including four-time *LAW360* privacy and data security practice group of the year. We represent businesses of all sizes, and in most industries, directly affected by the California Consumer Protection Act (CCPA). During counseling of clients on CCPA preparedness, we have identified various questions, ambiguities and issues that could be addressed through the attorney general's (AG) broad regulatory authority under the CCPA. We outline some of those and organize our comments by reference to the applicable sections of the CCPA that provide the AG rule-making authority. These comments do not necessarily reflect the opinions or concerns of all of our clients, and not all of our clients that have contributed to these comments necessarily join in all of them. These comments also do not reflect a position statement by the firm.

I. RULE-MAKING

A. Under its authority pursuant to Section 1798.185 (a)(4), the AG should promulgate rules and procedures as follows:

- "To facilitate and govern the submission of a request by a consumer to opt out of the sale of personal information pursuant to paragraph (1) of subdivision (a) of Section 1798.145 [sic]."[1] (Section 1798.185(4)(A).)

[1] The correct reference would seem to be to .135(a)(1).

- While changing the text of the homepage link might seem to require legislative action,[2] Section 1798.185(a)(b) supports the AG's authority to promulgate regulations that further the purposes of the title by providing businesses with the flexibility to use different language indicative of data subject rights and choices (e.g., "Privacy Choices") or add text to give broader application (e.g., "Privacy Choices (e.g., Do Not Sell My Personal Information"), and giving businesses the flexibility to have that link resolve to a privacy rights and choices page that provides notices and choice tools in addition to the CCPA's "do not sell" right for California consumers (i.e., a data subject rights management portal). This would further the overall purposes of the title – namely, effectively and efficiently informing consumers of their privacy rights and making it easy for them to understand and exercise those rights. The AG could also harmonize CCPA homepage notices with Shine the Light Act homepage notices under such a general choices link, which would also further the overall purposes of the title.

- "To govern business compliance with a consumer's opt-out request." (Section 1798.185(4)(B).)
  - Section 1798.115(d) governs the obligations on a third party regarding personal information that has been sold to it: "A third party shall not sell personal information about a consumer that has been sold to the third party by a business unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt-out pursuant to Section 1798.120." Section 1798.120 provides for a business' do-not-sell notice and request response obligations. However, since the recipient of sold personal information (i.e., the buyer) might not meet the definition of a business, and .120 does not mention the obligations of buyers (i.e., third-party recipients) of sold personal information, it is not clear that the obligations of .120 apply to all buyers (i.e., a third party that is not also a business) of personal information in a sale, and might even be read as imposing the obligation to stop downstream sales absent notice and opportunity to opt out on the selling business, after it receives a do-not-sell opt-out, rather than on the buyer. The AG could resolve this ambiguity and clarify that upon a sale, the obligations under .115(d) and .120 apply solely to the buyer (i.e., party that received the personal information via a sale) and not to the seller. While the seller may agree with the buyer to pass through the buyer's notice and opt-out opportunity, it should not be

[2] If the AG concludes so, it is suggested that the AG seek amendment to permit more flexibility in the text of the homepage link to data subject rights information and tools, especially since there may be many other states that follow with their own consumer privacy laws that may differ from the CCPA, and that such amendment revise Section 1798.83(b)(1)(B) of the Civil Code to have such link also satisfy the homepage link provisions of the Shine the Light Act. A better way to distinguish between a general privacy policy and special data subject rights under the CCPA, and other laws, would be "Privacy Choices" or something similarly simple and generic.

required to do so, and it should not be liable if the buyer should improperly engage in downstream sales without doing so.
    - The do-not-sell right, sometimes referred to in the title as an opt-out, is an opt-in for children under age 16 as set forth in Section 1798.120(c). That section refers to "consumers between 13 and 16 years of age" to refer to the group of children who can exercise that right themselves as opposed to having the consent exercised by parent or guardian. The AG should clarify that this means from age 13 to age 16 and not merely 14- and 15-year-olds; otherwise, 13-year-olds are left out entirely.

- "For the development and use of a recognizable and uniform opt-out "button" by all businesses to promote consumer awareness of the opportunity to opt out of the sale of personal information." (Section 1798.185(4)(C).)
    - Use of this button should satisfy the homepage and privacy notice "Do Not Sell My Personal Information" link obligations,[3] as long as that link is on the first page to which the button resolves.
    - Since the CCPA does not pre-empt the Shine the Light Act, this button could also be deemed to satisfy the "Your CA Privacy Rights" homepage link provisions,[4] as long as that link is on the first page to which the button resolves.
    - The button should be short and simple (e.g., "Privacy Choices") and be permitted to apply to more than just California if desired by the business.

B. "Establishing rules, procedures, and any exceptions necessary to ensure that the notices and information that businesses are required to provide pursuant to this title are provided in a manner that may be easily understood by the average consumer, are accessible to consumers with disabilities, and are available in the language primarily used to interact with the consumer, including establishing rules and guidelines regarding financial incentive offerings, within one year of passage of this title and as needed thereafter." (Section 1798.185(a)(6)).

- Businesses will struggle to meet the pre-collection notice requirements of Section 1798.100 (b) unless the AG provides that compliance with this requirement shall depend on the practicality of providing notice given a collection method and medium. For instance, it should be reasonable and sufficient notice to (1) rely on notices in online privacy notices on homepages or app settings menus for all data practices described therein via that online service, and (2) to allow other parties collecting personal information in connection with such online services to pass notices through to users via a service operator by including notice of and links to that other party's privacy notice in the operator's privacy notice, provide a URL address to an online privacy policy where written notice is impractical (e.g., call

[3] Section 1798.135(a)(1).
[4] Civil Code Section 1798.83(b)(1)(B).

center audio disclosures at the beginning of a call, or in text, chat app and other short-form communications), and provide signage at brick-and-mortar locations (e.g., surveillance cameras, point-of-sale devices).

- The provisions regarding reasonable financial incentive, and reasonable differential pricing and services, exceptions to the prohibition on discrimination based on CCPA rights exercise of Section 1798.125(a)(2) and (b)(1) discuss reasonableness in context of "value provided to the consumer by the consumer's data." This arguably suggests a consumer-specific subjective determination, which would be practically impossible. To meet the purposes of the title, the AG's regulations could specify that this value determination can be met by any reasonable objective measures, including costs and benefits to the business itself, and that where there is no good objective measure, the mere offering of a choice to consumers should be presumptively reasonable.

C. "Establishing rules and procedures to further the purposes of Sections 1798.110 and 1798.115 and to facilitate a consumer's or the consumer's authorized agent's ability to obtain information pursuant to Section 1798.130, with the goal of minimizing the administrative burden on consumers, taking into account available technology, security concerns, and the burden on the business, to govern a business's determination that a request for information received by a consumer is a verifiable consumer request, including treating a request submitted through a password-protected account maintained by the consumer with the business while the consumer is logged into the account as a verifiable consumer request and providing a mechanism for a consumer who does not maintain an account with the business to request information through the business's authentication of the consumer's identity, within one year of passage of this title and as needed thereafter." (Section 1798.185(a)(7).)[5]

- Businesses should be given broad flexibility in designing verification policies and procedures that are reasonably designed to minimize the need to collect any additional personal information beyond what has already been collected and to disregard or deny requests that cannot be reasonably verified based on such data limitation principle. To the extent the regulations require collection of additional personal information to verify a requesting party's identity or residency, the regulations should provide that the business may maintain that information for record keeping.

[5] "'Verifiable consumer request' means a request that is made by a consumer, by a consumer on behalf of the consumer's minor child, or by a natural person or a person registered with the Secretary of State, authorized by the consumer to act on the consumer's behalf, and that the business can reasonably verify, pursuant to regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185 to be the consumer about whom the business has collected personal information. A business is not obligated to provide information to the consumer pursuant to Sections 1798.110 and 1798.115 if the business cannot verify, pursuant this subdivision and regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185, that the consumer making the request is the consumer about whom the business has collected information or is a person authorized by the consumer to act on such consumer's behalf. (Section 1798.140(y))."

- To the extent the AG promulgates regulations providing what constitutes sufficient verification, businesses should be provided a safe harbor from any liability that might arise out of following such regulations (e.g., claims by a data subject that was impersonated by a party that was able to meet the verification standards of the regulations).

D. "The AG may adopt additional regulations as necessary to further the purposes of this title." (Section 1798.185(b).)

- The definition of "consumer" can be read to include nonconsumers such as employees, contractors and business-to-business contacts. This seems inconsistent with the consumer protection purposes of new Title 1.81.5 and conflicts with the existing California privacy and security provisions in Title 1.81 that it supplements, as well as other California privacy law. This could be resolved by further refining the definition of "consumer" to harmonize it with "customer" as defined in Title 1.81 (Data Records; Security and Breach)[6] and in the Shine the Light Act provisions thereof,[7] and/or "consumer" as defined by the California Online Privacy Protection Act.[8] Our clients have expressed myriad likely unintended consequences if employees can be read into the definition of consumer, including providing access to security logs, general email databases and confidential information. We note that the legislature has carefully crafted employee rights to access their personal information under the Labor Code to balance the interests of employees, businesses and other parties. An expansion of the definition of consumer to include employees and contractors would disrupt this balance and would not further the purpose of the title.

- The use of the undefined term "households" creates problems when used in the definition of personal information. It could be read to suggest that a consumer is entitled to access to and copies of personal information of household members, which would violate those members' privacy. Use of "household" in Section 1798.140(c)(1)(B) suggests that personal information on non-California residents is to be counted toward the 50,000 pieces of personal information collected that is required in order to meet business coverage thresholds. The same problem

[6] "Customer" means an individual who provides personal information to a business for the purpose of purchasing or leasing a product or obtaining a service from the business. Civil Code Section 1798.80(c).
[7] "'Customer' means an individual who is a resident of California who provides personal information to a business during the creation of, or throughout the duration of, an established business relationship if the business relationship is primarily for personal, family, or household purposes." Civil Code Section 1798(e)(1). "'Established business relationship' means a relationship formed by a voluntary, two-way communication between a business and a customer, with or without an exchange of consideration, for the purpose of purchasing, renting, or leasing real or personal property, or any interest therein, or obtaining a product or service from the business, if the relationship is ongoing and has not been expressly terminated by the business or the customer, or if the relationship is not ongoing, but is solely established by the purchase, rental, or lease of real or personal property from a business, or the purchase of a product or service, and no more than 18 months have elapsed from the date of the purchase, rental, or lease." Civil Code Section 1798(e)(5).
[8] "The term 'consumer' means any individual who seeks or acquires, by purchase or lease, any goods, services, money, or credit for personal, family, or household purposes." Business and Professions Code Section 22577(d).

applies to the use of the term "devices" without reference to California residents. The AG's regulations must provide clarity needed to resolve these issues.

- The CCPA is internally inconsistent as to whether or not the online notice needs to include the categories of sources from which personal information is collected, the categories of third parties to which personal information is disclosed and the specific pieces of personal information collected about a specific consumer. This should be clarified. Obviously, the last could not practically be done in a general notice, and doing so would be contrary to the privacy purposes of the title.

- Businesses must list the categories of personal information disclosed for a business purpose in the preceding 12 months (or if the business has not disclosed consumers' personal information for a business purpose in the preceding 12 months, the business must state that). However, there is no obligation to include a list of categories of personal information disclosed for a commercial purpose in the preceding 12 months. This distinction between the underlying purposes does not apply with respect to categories of personal information collected; it applies only to categories of information disclosed. The AG could clarify that there is no need to provide categories of personal information disclosed for a commercial purpose.

- The CCPA permits transfers to a third party of personal information of a consumer as an asset that is part of a merger, acquisition, bankruptcy or other transaction in which the third party assumes control of all or part of the business, provided that information is used or shared consistently with Sections 1798.110 and .115. If the recipient in such a transaction materially alters how it uses or shares the personal information of a consumer in a manner that is materially inconsistent with the promises made at the time of collection, it needs to provide to the consumer prior notice of the new or changed practice. However, Sections 1798.110 and .115 are the sections that set forth notice and disclosure requirements of consumer rights under the CCPA regarding businesses that collect personal information, sell personal information or disclose personal information for a business purpose. Presumably, the intent is that the data will continue to be used and shared as described in the privacy policy or notice that included those CCPA rights disclosures. The AG's regulations could confirm that and resolve the current ambiguity.

- The definition of business includes "[a]ny entity that controls or is controlled by a business, as defined in subparagraph (1), and that shares Common Branding ['shared name, servicemark, or trademark'] with the business." As such, the CCPA essentially requires all the members of a similarly branded family of companies that have an entity that meets the definition of a business to also be treated as a covered business. It is arguably not clear whether the intent is that the commonly branded entities must or can be treated as a single business under the

CCPA. The AG should clarify that the intent of Section 198.140(c)(2) is only to bring such an entity under coverage as a business even if it would not otherwise meet the conditions of .140(c)(1)(A)-(C). The AG's regulations could further clarify that such a business, or any other affiliate or subsidiary of a business, may elect to "roll up" to be treated as a single business, or to be separately treated as a distinct business, for CCPA purposes, so long as each business meets the controller requirements of .140(c)(1)(i.e., "determines the purposes and means of the processing of consumers' personal information"). In this regard, a family of companies is treated as a distinct business for CCPA notice and consumer rights response purposes if there is unitary control of the group's consumer personal information, but if affiliates maintain independent control they are separate businesses for CCPA purposes.

- Section 1798.140(c)(1) does not address what happens when a company meets one of the thresholds of (A)-(C). Given the title's 12-month look-back provisions, this could create an impossible burden for a business if application were immediate when a company that was not previously subject to the title later becomes subject. The AG's regulations could provide a grace period for compliance, such as beginning 12 months thereafter.

- The definitions of "business," "collect" and "sale" need to be reconciled when it comes to who is responsible for a business or other party collecting personal information in a manner that has some association with another business or its consumers. Examples include a solicitation firm collecting consumer personal information (e.g., for petitions or product marketing) on the property of a retailer (e.g., in front of the store or even at a booth in-store) or a cookie operator collecting IP addresses and other data from visitors to a retailer's website on which the cookie is associated. Because the definition of sale is "making available … a consumer's personal information" and not "making available access to a consumer from whom personal information is collected by another party," the determinative factor should be which party controls the actual collection, not the access to the consumer. In both cases above, the solicitor and the cookie operator control the means and methods of collection, even though they would not be able to collect the personal information but for the ability to reach out to the retailer's consumers. This interpretation is consistent with the purpose of the title – namely, to make controllers responsible for the data they collect and control. To take a broader interpretation could have many unforeseen consequences. Practically, some parties controlling certain data collection, such as the cookie operator, may need to pass their pre-collection and other notice obligations through to the consumer with the assistance of another party, such as the website publishers on whose sites they associate their cookies, but that is a matter of the controlling collector implementing its obligations and not of which party controls the means and methods of collection. If the AG were to conclude

otherwise, then it should make its interpretation clear given the current ambiguity regarding this important issue.

- Under the CCPA, "sell," "selling," "sale" and "sold" are defined as "selling, renting, releasing, disclosing, disseminating, making available, transferring or otherwise communicating a consumer's personal information to another business or a third party for monetary or other valuable consideration." Section 1798.140(t)(1). Arguably, any arrangement or agreement between two parties has to have an exchange of valuable consideration in order to be valid, and the proposition that personal information has value is arguably inherent in the title. Accordingly, the AG could resolve ambiguity regarding under what circumstances non-monetary consideration would make a disclosure of personal information a sale. Further, even monetary consideration should not trigger a transaction that includes the transfer of personal information as being a sale unless the consideration (monetary or otherwise) is directly attributable to, and in direct consideration for, the acquisition of personal information for the buyer's own commercial purposes, as opposed to other business arrangements where the personal information is not the direct subject of the exchange of consideration. For instance, the definition of third party specifically excludes third parties that do not meet the requirements of the definition of service provider (Section 1798.140(v)), which receive personal information for a business purpose pursuant to a contract that limits the use to providing services to the disclosing business for such business purposes and includes other usage and disclosure limitations and a specific certification of compliance. (Section 1798.140(W)(2).) However, unlike qualifying service provider disclosures that are carved out of the definition of sale at Section 1798.140(t)(2)(C), these exempt third-party disclosures are not specifically carved out of the definition of a sale. The engagement by a business of such a vendor has to have an exchange of consideration in order to be valid. That cannot logically mean, however, that a disclosure to such an exempt third-party vendor, where the title's contractual and certification requirements are met, is a sale because there was consideration to support the engagement. Rather the only logical interpretation of consideration (monetary or nonmonetary) for the purpose of designating a transaction as a sale is where (1) the recipient is allowed to use the personal information for its own and/or third-party commercial purposes; and (2) the consideration is given directly in consideration of the recipient's ability to use the personal information for its own and/or third-party commercial purposes. At a minimum, the AG's regulations should clarify that disclosure to a party exempt from the definition of a third party under Section 1798.140(t)(2)(C) is not a sale.

- A business does not "sell" personal information under the CCPA when a consumer uses or directs the business to intentionally disclose personal information or uses the business to intentionally interact with a third party, provided the third party does not also sell the personal information, unless that

disclosure would be consistent with the provisions of the title. (Section 1798.140(t)(2)(A).) However, a business cannot control what the recipient does or does not do. In order for this provision to be relied on, the AG's regulations could provide that a business may rely on a commitment from the recipient not to sell the personal information, unless otherwise consistent with the title, in facilitating a consumer's directions to a business to share personal information.

- The CCPA will regulate "personal information," broadly defined as "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*." (Section 1798.140(o).) Arguably, all data about a person is *capable of being associated with* a particular consumer or household. For instance, demographic data (e.g., gender, profession, race) is capable of being associated with a person, but alone, it will not reasonably enable their identification or be reasonably linked to a specific person. Compare this with the definition of personal information under Title 1.81 of the California Civil Code, which includes California's customer records security and breach laws, and the Shine the Light Act's marketing transparency and choice requirements. In that title, there is a top-level definition of personal information that includes "any information … capable of being associated with a particular individual" to which the duty of reasonable security under the circumstances applies, but more narrow definitions are used regarding a customer's rights regarding sharing for third-party marketing purposes ("any information *that when it was disclosed identified, described or was able to be associated with* an individual….)" and regarding the type of data that will trigger a breach notification obligation (first initial or name and last name plus an account number or ID number and password). While a broad definition arguably has utility with respect to providing notice of what data is collected, when applied to what data is disclosed or sold, and even more so as applied to opt-out, portability and deletion rights, it is practically unworkable. This problem is made worse by the CCPA's ambiguities regarding deidentified data and aggregate consumer information, discussed below. The AG's regulations could resolve this issue and further the purposes of the title by clarifying that "capable of being associated with" means "is able to be associated with an individual in the context of its use or disclosure."

- The definition of personal information under the CCPA does not include publicly available information. (Section 1798.140(o)(2).) "Publicly available" is defined as "information that is lawfully made available from federal, state or local government records, *if any conditions associated with such information*." (emphasis added.) The italicized language seems to be a typo or an incomplete thought that the AG's regulations could complete. Further, under the title, information is not "publicly available" if that data is used for a purpose that is not compatible with the purpose for which the data is maintained and made available in the government records or for which it is publicly maintained. Under the

Freedom of Information Act and state equivalents (e.g., California Public Records Act), all but the most sensitive government records are available to the public for any purpose. Because the uses by a business of public information may differ from the exact government collection purpose (e.g., property title records to establish land chain of title, but used by business for marketing or fraud prevention purposes), a narrow interpretation of this definitional carve-out from personal information would be inconsistent with our system of public access to government records. The AG's regulations could clarify that any purpose for use of government records not prohibited by applicable law is a compatible purpose for purposes of .140(o)(2).

- Also included in .140(o)(2)'s provisions regarding what is not personal information is deidentified data and aggregate consumer information, suggesting that these types of data are intended to be excluded from the definition of personal information, but this is unclear as the title is currently worded. The CCPA states "'Publicly available' does not include consumer information that is Deidentified or aggregate consumer information." The intent is likely to have used "personal information" rather than "publicly available," given the context. Further, Section 1798.145(a)(5) provides that "[t]he obligations imposed on businesses by this title shall not restrict a business's ability to … collect, use, retain, sell or disclose consumer information that is deidentified or in the aggregate consumer information." This would seem sufficient to remove deidentified and aggregate consumer information from the data applicable to deletion and do-not-sell rights. Practically, portability rights would also not apply, especially since the CCPA provides that there is no obligation to re-identify deidentified data "not maintained in a manner that would be considered personal information." However, the other obligations regarding personal information would seem to apply unless the definition of personal information is not clarified to exclude deidentified and aggregate consumer information, which would seem consistent with the intent and purposes of the title. Also, the definition of deidentified suffers from the same problem as the definition of personal information – data "capable of being associated with … a particular consumer," which could be cured by taking a narrower approach as already suggested as regards personal information.

- Section 1798.130(a)(2) provides the detail on how to comply with the data portability right outlined in Section 1798.100(d). Section .130(a)(2) provides that the data portability covers only the prior 12 months, i.e., anyone holding an account for more than 12 months preceding the request. However, .100(d) does not include that limitation. The AG should clarify that .130(a)(2) qualifies .100(d) and that they are not independent disclosure obligations.

- Section 1798.105(b) provides broad exceptions to a consumer's deletion rights under Section .105(a), including broad "catchall" provisions in subsections (7)

and (9). However, like most catchall provisions, the broad language lacks clarity and the AG could provide guidance as to what would and would not be included therein. It is suggested that in doing so, regulations apply the concept of legitimate interest and provide that any retention based on a good faith belief in a legitimate interest for retention shall be permissible so long as the use is limited to that purpose.

- Section 1798.150(a)(1) provides a limited private cause of action for certain types of, but not all, data security breaches (reference is made to a more narrow definition of personal information under Title 1.81 used there for breach notification purposes) in the case of "unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices." The AG's regulations should clarify whether "unauthorized" applies to all the following conditions, or only some (i.e., whether it applies to both access and disclosure). The AG's regulations could also clarify the cure provisions of Section 1798.150(b). The CCPA has no express duty regarding data security; those are in Title 1.81. Thus, the reference to the consumer notice to the business of "the specific provisions of this title the consumer alleges have been or are being violated" and an opportunity to cure that breach is confusing -- a remnant of an earlier broader private right of action that was rejected during the legislative process. The AG's regulations could rectify this by providing that this means providing notice of the alleged unreasonable security that allegedly resulted in the alleged triggering incident. Further, a consumer's CCPA cause of action is limited to data security failures that resulted in a breach, so it would seem that the only way to provide a meaningful opportunity to cure would be to rectify the security inadequacy on a prospective basis, since retrospective cure is an impossibility. This interpretation is also the only way to give purpose to the provision that the cure be documented by a written remediation and prospective compliance commitment, and that a breach of that written cure statement will revive the ability to seek statutory damages. The AG's regulations can clarify the intent of this provision and better detail the process for cure.

- Section 1798.155(a) provides the right of businesses to seek the opinion of the AG for guidance on how to comply with the title. It is suggested that the regulations provide that if a business does so and articulates a good faith basis for an interpretation of the title, the AG may not bring an enforcement action based on a contrary interpretation until 30 days after it has given the business notice of the contrary interpretation and a demand to cure. In addition, it is suggested that the regulations provide that the cure notice that the AG is required to provide a business under Section 1798.155(b) before the AG is authorized to commence an enforcement action include a reasonable description of what is required of the business to effect a sufficient cure. Such regulations guiding the opinion and

notice of cure obligations of the AG further the purpose of the title by prioritizing compliance (i.e., "fix it") over punishment (i.e., "gotcha"), especially as to businesses that can be shown to have acted in good faith.

- Given that the enforcement delay is until the earlier of July 1, 2020, or six months from the promulgation of the final regulations, and the AG has until July 1, 2020, to issue final regulations, it is possible that enforcement could commence with little or no time between the date the regulations are finalized and commencement of enforcement. Accordingly, it is suggested that the regulations provide for a further enforcement delay of six months from the final regulations with respect to any issue that is based on the regulations as opposed to clear from the four corners of the title.

II. CONCLUSION

We appreciate the opportunity to make comments for your consideration and look forward to participating in the formal rule-making process. If you have any questions regarding these comments, please feel free to contact me at 310.860.8860.

Respectfully submitted,

Alan L. Friel
Partner