




OOPS! And Other Takeaways from the First Draft of CPRA Regulations

By: [Kyle Fath](#), [Alan Friel](#) and [Shea Leitch](#)



On Friday, May 27, just a day after holding a public meeting where it hinted at providing a timeline for release of the draft but provided no indication that it would be dropping the Regs the next day, the California Privacy Protection Agency (“CPPA” or “Agency”) released a first draft of proposed regulations (“Regs”), a copy of which is available [here](#). You can read FAQs regarding the Agency’s rulemaking process and the Statement of Reasons published by the Agency in connection with the draft Regs [here](#) and [here](#). While the draft Regs do provide an indication of what the Agency’s priorities may be, they certainly are incomplete. The document purposely omits regulations on key topics, including automated decision-making and profiling, cybersecurity audits, and risk assessments (which the Agency announced would not be included in the first draft during its May 26 meeting), so we can expect the Regs to expand far beyond their current 66-page length. In addition, these draft Regs are non-final, as they are subject to consideration and a vote in the CPPA’s [June 8 meeting](#), followed by a period for public comment.

Most Notable Features of the Regulations

Below we provide an overview of some of the most notable features of the draft Regs:

Opt-Out Preference Signal; Do Not Sell/Share.

The CPRA includes a Global Privacy Control concept referred to as the “opt-out preference signal” (or “OOPS”). Though the statute makes honoring OOPS optional (see Section 1798.135(b)(3) of the statute (“A business that complies with subdivision (a) [i.e., by including opt-out links] ... is not required to comply with subdivision (b) [i.e., honoring OOPS]”) and Section 1798.185(a)(20)(referring to an election to comply with (b)), the Agency has decidedly taken the position that honoring OOPS is mandatory. Section 7025(e) and 7026(a)(1). The Agency appears to be hanging its hat on its new concept of processing OOPS signals in a “frictionless manner”—i.e., if your business processes OOPS in a frictionless manner it can forgo the opt-out links and mechanism, but if it does not then it must have both the opt-out links and mechanism and have a process for honoring OOPS, though that may involve certain steps and conditions, as discussed in further detail in the next paragraph. Regs. Sections 7013(d), 7025 (but compare to Section 7026(a)(1), which requires, at minimum, two methods in conflict with Section 7013(d) and 7025(e)). This approach is certain to receive a lot of comments and, should it become final, likely judicial challenge.

WTF is a “Frictionless Manner”?

To be considered to have honored a OOPS signal in a frictionless manner, the business must not: (1) Charge a fee or require any valuable consideration if the consumer uses an opt-out preference signal; (2) Change the consumer’s experience with the product or service offered by the business; or (3) Display a notification, pop-up, text, graphic, animation, sound, video, or any interstitial content in response to the opt-out preference signal (however, the business is permitted to present a pop-up or other notification asking for consent to ignore the OOPS). Therefore, for example, publishers will still have the opportunity to monetize content and present pop-ups in the way that is currently done when they detect a pop-up blocker. Section 7025(f).

The criteria for a “frictionless manner” comes from what the statute tasks the Agency to determine are part of the specification for the OOPS at 1798.185(a)(20) so there is a basis for requiring the OOPS to be “frictionless,” however, that does not necessarily mean that Section 1798.135 does not permit publishers to elect between links or frictionless OOPS. In addition, to qualify under Section 7025(g) to avoid having to post the DNSale NShare link and mechanism, the frictionless OOPS must also act as a consumer opt-out of offline sales and sharing if the business has the ability to link the signal to offline consumer data (e.g., the website visitor is logged in and thereby tied to their profile). It is not clear what is meant by “offline” as it is not defined in the Regs or the statute. Finally, it is proposed that third party controllers (e.g., cookie operators) collecting personal information on a first party business’ website are also required to look for and honor OOPS. Section 7052(c).

What can the opt-out link(s) say?

In terms of what links may be used, the Regs provide that they can either state: (1) “Do Not Sell or Share My Personal Information” and, if applicable, “Limit the Use of My Sensitive Information;” (2) Your Privacy Choices; or (3) Your California Privacy Choices; however, “this alternative opt-out link is to provide businesses the option of providing consumers with a single, clearly-labeled link that allows consumers to easily exercise **both** their right to opt-out of selling/sharing, and the right to limit, instead of posting the two separate [links] ” (emphasis added). That begs the question: can a company that does not use or disclose sensitive personal data in a manner that is subject to limitation still take advantage of the alternative link to address sale/share? Given that some sort of conspicuous opt-out link will be required for the other 2023 state privacy laws (e.g., Colorado, Virginia), option 2 would seem to present a clean and consumer friendly way of pointing consumers to their various opt-in and opt-out options. To emphasize, however, if the proposed OOPS provision is not reworked the processing of opt-out preference signals would still be required, they would just seemingly not have to be in a “frictionless manner.” See Sections 7013(b) and 7015(b).



Combined DNSell/DNShare Requests?

The Agency appears to treat the separate opt-out from sale and sharing rights as a single, combined obligation to a business. In other words, if a business receives a “Do Not Sell” request it must also treat it as a “Do Not Share” request, and vice versa. A number of sections, including the new definition of “Opt-Out of Sale/Sharing” indicate that the Agency is not bifurcating the concepts and will seemingly require businesses to treat one as both. See, e.g., Sections 7001(z) (“neither sell nor share”), 7025(c) and 7026, among others.

While the statute speaks in terms of a combined DNSale or DNShare link, it provides that such link be “to an internet webpage that enables a consumer ... to opt-out of a sale or sharing...” (emphasis added). It is conceivable that some consumers may want to opt-out of sale, but not sharing for cross-context behavioral advertising, or vice versa, and the conflation of these rights in the Regs would prevent that. This, too, is likely to receive comments, assuming the full Agency Board even votes the provision forward. Furthermore, the Regs require DNSell / DNShare opt-outs to be flowed down to third party sale / share recipients, who must honor the opt-out in the same manner as the business. Section 7052(a). There is no express authority in the statute for such a pass through of opt-outs.

No OOPS Technical Details.

Setting aside the controversy of the requirement (or lack thereof) of processing OOPS signals, the Agency provided no technical requirements on opt-out preference signal or regulations touching on the statute’s requirement that the signal must be sent with a consumer’s consent, which would likely require it to be a user-enabled rather than a default setting. In addition, the Regs provide no details on how a business can and should determine residency with respect to an OOPS signal. While we need significantly more detail on this, and as the debate regarding the optional nature of OOPS rages on, a few other interesting aspects the OOPS-related Regs worth raising include: (1) effectively requiring businesses to tie an OOPS opt-out to non-cookie and other non-online information where a consumer is signed into the business’ account online (but not if the consumer is not signed in) (Section 7025(c)(7)(A)-(B)); and (2) displaying an online message as to whether the business has “Honored” the OOPS opt-out for a particular device/consumer (Section 7025(c)(6)). In addition, the Regs not applying the OOPS to limitation of sensitive information, as the statute provides, alone arguably causes the current proposal on OOPS to fall short of the statutory requirements.



Principles Regarding Consumer Requests and Consent.

In addition to the specific requirements regarding the various consumer request types discussed below, the Agency outlined several overarching requirements applicable to all types of consumer requests. Among these general requirements, businesses must:

1. Ensure the consumer request methods and accompanying instructions are easy to understand;
2. Offer symmetry in choice. In other words, “[t]he path for a consumer to exercise a more privacy protective option shall not be longer than the path to exercise a less privacy-protective option.”
3. Avoid confusing language (including double negatives).
4. “Avoid manipulative language or choice architecture.”
5. Be easy to execute.

Section 7004(a). Failure to comply with the requirements above may be considered a “dark pattern” under the CPRA. Additionally, the Regs clarify that “[a] user interface is a dark pattern if the interface has the effect of substantially subverting or impairing user autonomy, decisionmaking [sic], or choice, regardless of a business’s intent.” Section 7004(b) and (c).



Right to Delete.

The draft Regs make explicit businesses’ obligations to flow down requests to delete to service providers, contractors, and third parties. Specifically, the Regs instruct businesses to notify contractors and service providers delete PI on request from an eligible consumer, and also require service providers and contractors to comply with those requests and pass the request down to subprocessors. Section 7022(b)(2) and (c). Additionally, third parties to whom a business has shared or sold PI must be instructed to delete the PI (Section 7022(b)(3)), and the Regs add that they must comply (Section 7052(a)). The former is required by the statute, but the latter is not explicitly stated.

Right to Correct.

The Regs’ provisions regarding requests to correct primarily revolve around issues of contested data, as well as how businesses are expected to effectuate correction requests. On the former point, the Agency instructs businesses to consider the “totality of the circumstances” when determining whether to accept new PI presented by a consumer, or to reject the request. Factors to consider include:

- (A) The nature of the personal information (e.g., whether it is objective, subjective, unstructured, sensitive, etc.).
- (B) How the business obtained the contested information.
- (C) Documentation relating to the accuracy of the information whether provided by the consumer, the business, or another source. Requirements regarding documentation are set forth in subsection (d).

Section 7023(b)(1). Helpfully, the Regs add that “[i]f the business is not the source of the personal information and has no documentation to support the accuracy of the information, the consumer’s assertion of inaccuracy may be sufficient to establish that the personal information is inaccurate.” Section 7023(b)(2).

With respect to the implementation of correction requests, the Regs advise that businesses should update the PI on existing systems, and also take measures to ensure that the information stays accurate. Essentially, the CPPA is telling businesses to make sure that corrected information is not subsequently overwritten by incorrect information. Additionally, businesses are obligated to pass along correction requests to contractors and service providers. Section 7023(c).

Limit the Use of My Sensitive Personal Information.

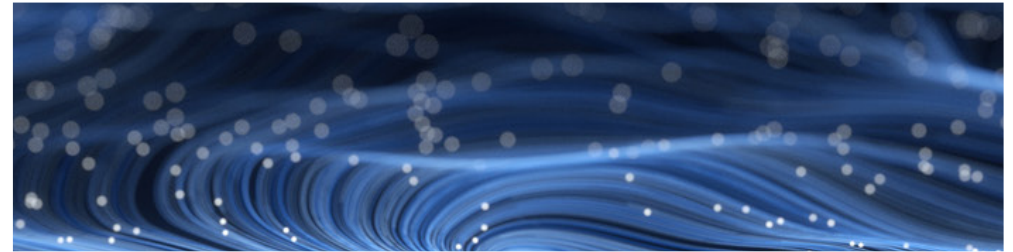
In a regulatory scheme rife with difficult acronyms, we have to compliment the Agency here for coining the phrase “right to limit” to refer to a consumer’s right to limit the use or disclosure of sensitive personal information. As promised by the statute, the Regs provide the purposes for which a business can use or disclose sensitive PI without offering the right to limit, including performing services reasonably expected by an average consumer, fraud prevention, ensuring physical safety of natural persons, short term transient use for nonpersonalized advertising, and other routine business purposes. In addition to enumerating such business purposes, the Agency provides helpful examples within each one. See Section 7027. The Regs also require that the privacy notice and retention schedule break out disclosure of sensitive personal information collected into the nine subcategories set forth in the statute.

Right to Know (access).

Consistent with the statute’s expansion of the lookback period for access requests beyond 12 months after January 1, 2022, the Regs do so, but clarify that they may limit such requests where compliance would involve disproportionate effort, measured by a balancing test of the time and resources against the benefit to the consumer. Section 7001(h) and 7024(h). “For example, responding to a consumer request to know may require disproportionate effort when the personal information which is the subject of the request is not in a searchable or readily-accessible format, is maintained only for legal or compliance purposes, is not sold or used for any commercial purpose, **and** would not impact the consumer in any material manner.” Section 7001(h)(emphasis added). However, failure to put appropriate systems in place to reasonably fulfill requests will negate a claim of disproportionate effort. *Id.*

Verification.

Interestingly, these regulations provide few revisions to the sections relating to verification of requests.



Purpose Limitation. “Reasonably Necessary and Proportionate” Defined.

The Regs provide helpful guidance on the purpose limitation requirements in the statute, namely, by defining “reasonably necessary and proportionate.” The Regs provide that this limitation means that collection, use, retention, and sharing of PI must be “consistent with what an average consumer would expect when the personal information was collected” or “for other disclosed purpose(s) if they are compatible with what is reasonably expected by the average consumer.” Section 7002(a). This section also provides examples of what may or may not be reasonably necessary and proportionate. However, the examples suggest that certain advertising and marketing practices, particularly regarding geolocation and third party marketing, would not be permissible without specific notice and express consent.

Notice at Collection.

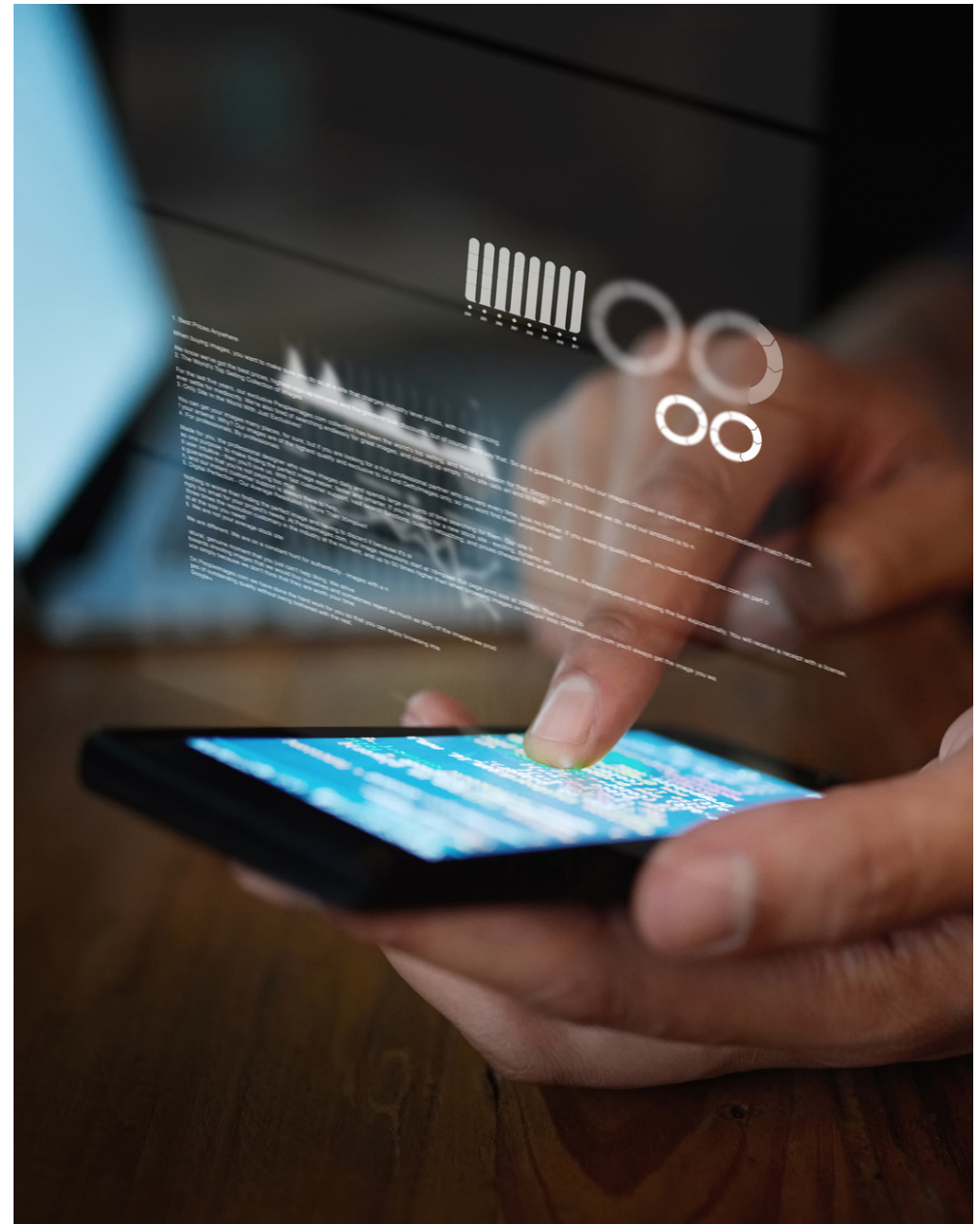
Along with the statutory additions to the notice at collection requirements—most notably, retention details on a category basis (and for sensitive personal information, subcategories)—the Regs have added significant substance, particularly as it relates to third parties controlling the collection on a first party’s website or premises. See Section 7012. In particular, the Regs require, among other things:

- The first party business to include in its notice at collection names of all such third parties, or in the alternative, information about the third parties’ business practices. Section 7012(g)(2).
- The third party businesses that control the collection on another business’s website or physical premises, such as in a retail store or in a vehicle, must still provide a notice at collection in a conspicuous manner, though it can do so as part of the first party’s notice (e.g., the first party provides notice at collection of where the third party’s notice can be found online). Section 7012(g)(1)-(4).
- However, these provisions explicitly do not relieve the first party of its obligations “to comply with a consumer’s right to opt-out of sale/sharing. If a consumer makes a request to opt-out of sale/sharing with the first party, both the first party and third parties controlling the collection of personal information shall comply with sections 7026, subdivision (f) (honoring opt-outs) and 7052, subdivision (a) (passing opt-outs down to the sale/share recipient). Section 7012(g)(1)(A).

There is no discussion on how this relates to the broadening of the exemption to sale/sharing under the statute where the consumer “uses or directs the business to: (1) intentionally disclose personal information; or (2) intentionally interact with one or more third parties,” Section 1798.140(ad)(2)(A) and (ah)(2)(A), and the Regs do not provide any guidance on this type of disclosure.

Notice of Financial Incentive.

While few changes and details are provided in relation to financial incentives (such as loyalty programs, discounts in exchange for email sign-ups, etc., which have been a focus of CCPA enforcement), the Regs remove the requirements of personal information valuation and explaining how that value is reasonably related to the program benefits, unless the program requires waiver of consumer rights to avoid a price or service difference. Sections 7016(d)(5), 7080 and 7081.





Service Provider, Contractor, and Third Party Management.

This first draft of the Regs perhaps hints at one of the Agency's potentially greatest area of focus, namely the management of data relationships. In short, the practice of papering relationships with a one size fits all template will not be sufficient in the eyes of the Agency. In addition, it is clearly focused on the "sale/share" issue on vendor-by-vendor (or other recipient) basis.

- *New Expanded Requirements.*

- Service Providers/Contractors. The Regs require very prescriptive contractual terms to designate a data recipient as a service provider or contractor, including identification of the specific business purposes and services for which the service provider or contractor is processing information. Further, the Regs specify that "[t]he description shall be specific" and "shall not be described in generic terms." As a result, businesses would not be able to apply generic provisions across what is sometimes thousands of vendors. On the flip side, vendors will have to be specific in contract templates about the business purposes and services involved. See Section 7051. Importantly, the Regs state that failure to meet these prescriptive requirements means that the recipient is not a service provider or contractor, and thus, a sale / sharing is occurring. Section 7051. In addition, the Regs, in keeping with the statute, require at least eleven specific contractual obligations to be valid. Beyond that, the Regs add non-contractual obligations that apply to service provider / contractors and their subprocessors.

- Third Parties (sale or sharing recipients). The agreement with statutorily-defined third-parties must identify "the limited and specified purposes for which the personal information is sold or disclosed" and "must not be described in generic terms", but rather "shall be specific." The contractual requirement is very strict; any third party is restricted from collecting, using, processing, retaining, selling, or sharing personal information from a business in the absence of a compliant contract. Section 7053. In addition, although not expressly provided for under the statute, the Regs add affirmative obligations on third parties, including the obligation to honor deletion and DNSale / DNShare requests made to a first party and passed down, and to look for an honor OOPS signals to a first party website on which they operate. Section 7052.

- *Diligence and Audits of Data Recipients.* The Regs certainly incentivize businesses to audit their vendors and other data recipients (a right which must be in contracts with service providers, contractors, and third parties): "[D]epending on the circumstances, a business that never enforces the terms of the contract nor exercise its rights to audit or test the [recipient's] systems might not be able to rely on the defense that it did not have reason to believe that the [recipient] intends to use the personal information in violation of the CCPA and these regulations...." Section 7051 and 7053.

- *Notice at Collection Requirements.* As discussed above, both first parties and third parties controlling the collection of personal information on a first party website or premises have notice at collection obligations with respect to the third parties' collection.

Enforcement.

The Regs contain a procedure for consumers to submit requests to the Agency, including the information that must be submitted in connection with a complaint. In its Regs, the Agency commits to notifying complainants “in writing of the action, if any, the Agency has taken or plans to take on the complaint,” as well as the Agency’s rationale for action or inaction. When the Agency initiates an enforcement action, it will issue a probable cause notice to the alleged violator. The Agency will conduct a Probable Cause Proceeding in a closed hearing (unless a public hearing is requested by the alleged violator at least 10 days prior to the proceeding), in which it will evaluate evidence presented by the alleged violator (with counsel) and the CPPA Enforcement Division. The Agency will issue a written Probable Cause Determination based on evidence presented, which will not be a public document. The decision “is final and not subject to appeal.” Section 7302. Alternatively, the Enforcement Division and the subject of the complaint may enter into a stipulated order, prior to the entry of a Probable Cause Determination, which will be a public document. Section 7303. Finally, the Regs also empower the Agency to conduct audits, “to investigate possible violations of the CCPA” and also where “the subject’s collection or processing of personal information presents significant risk to consumer privacy or security, or if the subject has a history of noncompliance with the CCPA or any other privacy protection law.” Section 7304. Presumably this means entities which have been subject to significant enforcement actions (for example, by EU supervisory authorities) may expect to be audited by the CPPA.



Notable Regs–Cookies and AdTech.

- *Non-First Party Cookies are deemed a sale or sharing if not qualified as service providers/contractors.* The Regs do not specifically state that the collection of personal information by third-party cookies on a first party site constitute a sale/sharing by the first party site. However, the statute changed the definition of third party to exclude service providers and contractors. The Regs provide that “[a] third party shall comply with a consumer’s request to delete or request to opt-out of sale/sharing forwarded to them from a business that provided, made available, or authorized the collection of the consumer’s personal information.” Section 7052(a). Further, the Regs make clear that a first party that allows third-party businesses to collect personal information are not thereby relieved from passing DNSale / DNShare opt-out to those third parties. Combined, this implies that absent an exception from sale / share, such as an express direction / interaction (i.e., opt-in) opt-outs apply to third party controllers such as third party cookie operators.
- *Cookie Banners alone are not sufficient for Do Not Sell/Share Opt-Outs.* While this point seems obvious given the growing reliance on cookieless technology and identifiers to target advertisements, it underscores a potential enforcement priority for the Agency of looking beyond facial compliance. The Agency emphasizes that cookie controls like cookie banners only address the “collection” and not the sale or sharing of personal information.
- *Turning off Cookies Will Not Be Sufficient for Honoring a Do Not Sell/Do Not Share Request.* In addition to its statements regarding cookie banners, the Regs require businesses to notify sale/sharing recipients of the request, and require such sale/sharing recipients to notify other downstream recipients, Section 7026(f) (3), and requires third parties to do so, Section 7052(a). In effect, the Regs require a signal-based opt-out system, much like the one that was developed by the Interactive Advertising Bureau (IAB) for the CCPA, and that such signal also trigger a downstream opt-out and not just a termination of ongoing sales / shares. It remains to be seen how organizations outside of the AdTech ecosystem will pass such signals or otherwise provide notifications in relation to DNSell / DNShare requests for more traditional types of PI.
- *Any use cases involving cross-contextual behavioral advertising will prevent a vendor from being considered a service provider or contractor.* In addition, routine activities that are able to fit under the service provider role under the current CCPA, such as custom audiences or email matching for advertising purposes, are stated explicitly in the Regs to fall outside of service provider permitted purposes (and thus would constitute a sale/sharing). Section 7050(c)(1).



Conclusion

While the Agency kicked some of the more difficult issues down the road for further consideration, its first draft of proposed Regs is quite comprehensive with respect to the issues addressed. The authority for some of what is proposed is questionable and will likely be challenged in comments, if not judicial action if such provisions become final. Interested businesses are encouraged to submit public comments. In addition to assisting specific clients and their trade organizations make comments, SPB plans on making comments based on unnamed clients that seek to be anonymous. While we will make it clear that such comments do not necessarily reflect the opinions or concerns of all of our clients we found during the CCPA rulemaking that this is a useful way for clients to get their views across when they are not comfortable doing so directly and lack a trade group that they can work through to get their views in front of the regulator.

For more information, contact the authors or your SPB relationship partner.

Contact Us



Alan L. Friel
Partner, Los Angeles
T +1 213 689 6518
E alan.friel@squirepb.com



Kyle Fath
Partner, Los Angeles
T +1 212 872 9863
E kyle.fath@squirepb.com

Colin Jennings
Partner, Cleveland

Kristin Bryan
Partner, Cleveland

Glenn Brown
Of Counsel, Atlanta

Shea Leitch
Of Counsel, Washington DC

Elizabeth Berthiaume
Associate, Dallas

Kyle Dull
Senior Associate, New York

Niloufar Massachi
Associate, Los Angeles

David Oberly
Senior Associate, Cincinnati

Gicel Tomimbang
Associate, Los Angeles



SQUIRE 
PATTON BOGGS

squirepattonboggs.com