Skadden

Privacy & Cybersecurity Update

CPPA Moves Towards Finalization of CPRA Regulations

Over the course of October and November 2022, the California Privacy Protection Agency (CPPA) issued revised draft regulations for the California Privacy Rights Act (CPRA), the law that amended the California Consumer Privacy Act (CCPA). If the CPPA determines that no further work is required, the agency's board will prepare a final rulemaking package to submit to the California Office of Administrative Law (OAL). On its present track, the final CPRA regulations will be published in late January or early February of 2023 at the earliest. Given that the final implementing regulations will therefore be published after the CPRA takes effect on January 1, 2023, the CPPA has indicated that enforcement may be delayed.

On October 17, 2022, the CPPA released modified proposed implementing regulations for the CPRA, as well as an explanation for such modifications, in advance of a board meeting that was held on October 28-29, 2022, during which the CPPA board reviewed certain of the proposed modifications to the draft regulations. On November 3, 2022, the CPPA released updated modifications to the proposed regulations, triggering a 15-day public comment period that ended on November 21, 2022.

If the CPPA determines that the no additional work is needed to finalize the regulations, then the agency will prepare a final rulemaking package, including draft final regulations and a final statement of reasons, to submit to the OAL. The OAL will then have 30 working days to approve or disapprove the regulations. Upon the OAL's approval, the draft regulations will become final.

Below, we cover three topics: (1) updated timing regarding the publication of the final CPRA regulations and related enforcement; (2) certain key incremental changes in the proposed modifications to the draft regulations released on October 17 and November 3; and (3) what topics remain outstanding for the CPPA regarding the CPRA regulations.

Expected Timing of Final Regulations and Enforcement

As mentioned previously, the CPPA board members noted during their meeting that they expect the current rulemaking process to conclude in late January or early February of 2023, which would mark a notable delay from the original deadline to finalize the regulations that had been set for July 1, 2022.[1] Furthermore, the rulemaking package

[1] Cal. Civ. Code §1798.185(d).

© Skadden, Arps, Slate, Meagher & Flom LLP. All rights reserved.

being considered will only be a partial set of regulations, as several topics have yet to be addressed in the draft regulations. Thus, even when the current set of proposed regulations are finalized, the CPPA will still need to engage in further rulemaking, with additional regulations to be expected.

The CPRA, as an amendment to the CCPA, goes into effect on January 1, 2023, with civil and administrative enforcement originally set to commence on July 1, 2023. However, the CPPA board discussed the need to act as a "reasonable enforcer" and provide leniency to businesses that have made good-faith efforts to comply with the regulations given the uncertainty regarding when the regulations will be finalized and the limited time remaining for businesses to adjust their compliance posture. Furthermore, the proposed modified regulations indicate that CPRA enforcement may be further delayed on a case-by-case basis. Specifically, the proposed regulations state that the CPPA "may consider all facts it determines to be relevant, including the amount of time between the effective date of the statutory or regulatory requirement(s) and the possible or alleged violation(s) of those requirements, and good faith efforts to comply with those requirements."[2]

Key Updates to the Draft CPRA Implementing Regulations

Clarification on Opt-out Preference Signals

The CPPA board proposed clarifications regarding opt-out preference signals during the board meeting, which were reflected in the proposed modifications to the regulations. Opt-out preference signals are signals set on behalf of a consumer — via a browser or other technology — to communicate the consumer's choice to opt out of the sale and sharing of their personal information. Three of the most noteworthy clarifications are described below:

- **Mandatory Requirement to Honor Opt-Out Preference Signals (§ 7025(b)):** While not a surprise — given the California AG's settlement with Sephora in September 2022 and the fact that the draft regulations from May 2022 took the position of making it mandatory that all businesses abide by opt-out signals — the CPPA board reemphasized that all businesses are obligated to comply with opt-out preference signals.
- **Opt-Out Applies Across Devices and to Pseudonymous Profiles (§ 7025(c)(1)):** Opt-out preference signals not only must be applied with respect to the specific browser or device being used by the consumer at the time that the signal is sent, but the signal also must be treated as a valid request to opt-out of sale/sharing for that consumer generally, where the business has a consumer profile associated with such browser or device — even where the profile is pseudonymous.
- **Financial Incentive Programs (§ 7025(c)(4)):** The CPPA board discussed (and the latest revisions to the draft regulations clarified) how a business should react when it receives an opt-out preference signal that conflicts with a consumer's participation in the business's financial incentive program that requires the consumer to consent to the sale/sharing of their personal information. The board determined that in such a situation, the business should notify the customer that processing the opt-out preference signal as a valid request would withdraw the consumer from the financial incentive program and let the consumer decide how to proceed. If the consumer affirms that they do intend to withdraw from the program, the business should process the signal as a valid opt-out request. If, however, the consumer either affirmatively opts to remain in the program or does not indicate any preference, then the business may ignore the opt-out preference signal. In the case where the business does not confirm the consumer's preference, the business is required to process the signal as a valid opt-out request.

Intent as an Element of Dark Patterns (§ 7004(c))

As noted in our June 2022 *Privacy & Cybersecurity Update*, the draft regulations include guidance regarding what constitutes a "dark pattern" — defined as a user interface that "has the effect of substantially subverting or impairing user autonomy, decision-making, or choice." The prior draft of the regulations clearly stated that a business's intent is irrelevant when determining whether a user interface constitutes a dark pattern. The updated regulations now provide that intent is a factor that can be considered, though a user interface may still be considered a dark pattern even if the business had no intent to subvert or impair user choice.

Exceptions to Notice Requirement for Sensitive Personal Information (§ 7014(g))

A business is generally required to inform consumers of their right to limit the business's use and disclosure of their sensitive personal information and to provide them with the opportunity to exercise this right. The previous draft regulations exempted from this requirement any business that only uses and discloses sensitive personal information for the purposes specified in Section 7027(m) of the regulations, and states so in its privacy policy. The updated draft regulations revised the list of exempt uses in Section 7027(m) and also now would consider a business exempt from the requirement if it only collects or processes sensitive personal information without the purpose of inferring characteristics about a consumer, and states so in its privacy policy.

[2] § 7301 (b), Modified Text of Proposed Regulations.

Elimination of Requirement to Identify Third Parties Collecting Personal Information on a Business's Behalf (§ 7012(e), (g)(1))

The previously proposed draft regulations included a requirement applicable to businesses that would allow third parties to control the collection of personal information. Such businesses were to be required to disclose, at or prior to the time of collection, either (1) the names of all such third parties or (2) information about such third parties' business practices. The obligation to include these details in such notice have been eliminated from the updated draft regulations.

The updated regulations also clarify that where a business allows one or more third parties to control the collection of personal information, all such parties would be permitted to provide a single notice at collection detailing the required information regarding their collective practices regarding the collection, use, disclosure, sale, sharing and retention of personal information.

When Service Providers Must Comply With Consumer Requests (§ 7050(g))

The updated draft regulations clarify how the CCPA's obligations to comply with consumer requests would apply in cases where a service provider is an entity providing services to a "nonbusiness" (*i.e.*, an entity that is not defined as a "business" under the CCPA). The proposed regulations would require the service provider to test whether it meets the requirements of the definition of "business" as defined in the CCPA. The regulations note that a service provider that is unable to determine how consumers' personal information is processed would not be considered a "business," whereas a service provider that uses consumers' personal information for the service provider's own purposes (*e.g.*, developing new products) may be considered a "business" that would be required to comply with consumer requests if received.

Clarifications Regarding Purpose Limitations and Secondary Uses of Personal Information (§ 7002(b), (c))

The CPRA requires that a business's collection, use, retention and sharing of a consumer's personal information be "reasonably necessary and proportionate to achieve [(1)] the purposes for which the personal information was collected or processed, or [(2)] for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes." The modified draft regulations provide guidance regarding both of these prongs.

Regarding the prong (1), the draft regulations would require that any purposes be "consistent with the reasonable expectations of the consumer." These "reasonable expectations" would be based on the following:

- the relationship between the consumer and the business;
- the type, nature and amount of personal information that the business seeks to collect or process;
- the source of the personal information and the business's method for collecting or processing it;
- the specificity, explicitness, prominence and clarity of disclosures to the consumer about the purpose for collecting or processing their personal information; and
- the degree to which the involvement of service providers, contractors, third parties or other entities in the collecting or processing of personal information is apparent to the consumer.

Regarding prong (2), the draft regulations specify that the determination would be based on the aforementioned "reasonable expectations" of the consumers, the other disclosed purpose for which the business seeks to further collect or process the consumer's personal information, and the strength of the link between the two.

Outstanding Topics for Future Rulemaking Activities

Still noticeably absent from the modified draft regulations is guidance regarding a variety of other topics that are mandated to be covered in the regulations, including:

- opt-out rights with respect to automated decision-making; and
- annual cybersecurity audits and privacy risk assessments for "businesses whose processing of consumers' personal information presents significant risk to consumers' privacy or security."

Given the CPPA's desire to finalize the CPRA regulations, these and other topics will likely be addressed in future rulemaking activities to be released in 2023.

While many had expected the CPPA to provide technical specifications for the aforementioned opt-out preference signals, the CPPA staff indicated during the board meeting that no such specifications would be forthcoming. The draft regulations currently include no meaningful technical specifications, with the only requirement being that the signal "be in a format commonly used and recognized by businesses. An example would be an HTTP header field or JavaScript object."

Key Takeaways

While the long-awaited CPRA regulations remain yet to be finalized, the CPPA has been moving more expeditiously to finalize them and aims to do so in late January or early February 2023. Even with the aforementioned delayed enforcement of the CPRA, 2023 will likely be a busy year for companies, as many will need to ensure the compliance with various comprehensive

privacy laws and regulations. In addition to the CPRA, comprehensive privacy laws also will be coming into force next year in Virginia (January 1, 2023), Colorado (July 1, 2023), Connecticut (July 1, 2023) and Utah (December 1, 2023).

Return to Table of Contents

FTC Settles Action Against Vonage Over Its Use of Dark Patterns and Junk Fees[3]

The Federal Trade Commission (FTC) and Vonage settled an action brought by the agency under the FTC Act and the Restore Online Shoppers' Confidence Act.[3] This settlement underscores the need for businesses to have clear, transparent and simple cancellation processes and billing policies when marketing and selling services to customers.

On November 3, 2022, the FTC announced that it had settled its action against Vonage, an internet-based communication services provider, following allegations that the company had engaged in illegal practices by artificially complicating its cancellation process and charging customers unexpected fees.

Background

Vonage advertises and sells phone services to both residential customers and small businesses. The company's phone plans automatically renew, which means customers are charged directly until they affirmatively indicate their desire to cancel by a specified date. The company stated that enrollment could be completed either through a toll-free phone number or through using the company's website, which required no interaction with a live agent. While the toll-free number option did require interaction with an agent, the phone number was prominently displayed at the top of each page on the Vonage website. The company also enrolls customers itself using "negative option" plans, which begin as a free trial but treat customers' subsequent inaction as consent to be charged.

Compared to the enrollment process, the FTC alleged that Vonage's cancellation process was extremely difficult.[4] According to the complaint, from 2017 to 2022, customers could not cancel their Vonage services online and also asserted that the exclusive method of cancellation that Vonage offered involved speaking over the phone with a live "retention" agent. According to the FTC, details about this cancellation method were buried in Vonage's terms of service. In addition, the complaint alleged that the cancellation process was further complicated because Vonage employed "dark patterns," which are interfaces and user experiences that lead users into making unintended, unwilling and potentially harmful decisions. These dark patterns included using a special cancellation phone number that had limited hours of operation, failing to provide requested callbacks, having excessive hold times and subjecting customers who wanted to cancel to aggressive sales pitches.

In addition to the onerous cancellation process, the complaint alleged that Vonage used fees to deter customers from cancelling their plans. Numerous customers were required to pay an "Early Termination Fee," also termed "junk fees," if they desired to cancel their contract with the company. The complaint stated that the amount and existence of the Early Termination Fee was obscured and therefore unknown to many residential and small business customers until they attempted to cancel their contract. Additionally, some customers who were able to complete Vonage's cancellation process allegedly continued to be charged for recurring service fees. According to the complaint, when these customers complained, they often received only partial refunds or no refund at all.

The Settlement

Pursuant to the proposed court order, Vonage agreed to pay $100 million in refunds to customers who have been harmed by its actions and adopt specific measures, including:

- **No Unauthorized Charges:** Requiring express, informed consent before charging customers.
- **Simplify Cancellation:** Simplifying its cancellation process so that it is easily accessible and efficient.
- **No Dark Patterns:** Stopping the use of dark patterns to deter customers from cancelling their plans.
- **Transparency of Terms:** Clearly disclosing the terms of negative option plans to customers, including any actions required to avoid being charged and the timeline in which such actions are required.

Key Takeaways

This enforcement action and settlement serve as a warning to companies regarding increased scrutiny by the FTC with respect to the use of dark patterns and junk fees. This trend is likely to continue, with other regulators in the U.S. and abroad giving greater attention to these harmful tactics, seeking higher fines to disincentivize such illegal activity.

Return to Table of Contents

[3] The details of the FTC's settlement can be found here.

[4] The FTC complaint can be found here.

UK Information Commissioner's Office Publishes Guidance on Direct Marketing Using Electronic Mail

The U.K.'s supervisory authority for data protection, the Information Commissioner's Office (ICO), published guidance on direct marketing via electronic mail (which has been broadly defined and includes emails, texts and direct messages via social media) in the U.K.

On October 18, 2022, the ICO published useful guidance titled "Guidance on Direct Marketing Using Electronic Mail," which provides clarity to organizations on various rules governing direct marketing via electronic mail. The guidance appears to be partially inspired by recent breaches of direct marketing rules and enforcement action taken by the ICO in the U.K.

Overview of Direct Marketing Rules in the UK

The Privacy and Electronic Communications Regulations 2003 (as amended) (PECR) implement the EU Directive on Privacy and Electronic Communications (Directive 2002/58/EC), which sets out the minimum requirements for direct marketing (including via electronic mail) in an EU member state. PECR forms part of the U.K.'s wider data protection regime governing direct marketing, which includes the U.K. GDPR and U.K. Data Protection Act 2018, and continues to apply post-Brexit as part of retained EU law. Additionally, PECR regulates several areas in relation to electronic communications, including marketing by electronic means (*e.g.*, calls, emails, texts, faxes) and the use of cookies or similar tracking technologies (*e.g.*, apps on smartphones).

The guidance refers to two key concepts that are defined in U.K. law:

- **Electronic Mail:** "Electronic mail" is defined under PECR as "any text, voice, sound or image message sent over a public electronic communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient and includes messages sent using a short message service." The guidance notes that this definition is intentionally broad to cover both existing and new forms of electronic mail, and includes email, text, picture, video, voicemail, in-app and direct social media messages.
- **Direct Marketing:** "Direct marketing" is defined in the U.K. Data Protection Act 2018 as "the communication (by whatever means) of advertising or marketing material which is directed to particular individuals," which includes all types of advertising, marketing and promotional materials (see examples in the "Consent," "Soft Opt-in" and "Viral Marketing" sections below). While this definition does not include messages sent for administrative or customer service purposes, often referred to as "service messages" (*e.g.*, email advice to a customer about an account issue), the guidance warns that any promotional content within a service message may amount to direct marketing. This was illustrated by the ICO fining Halfords Limited £30,000 in September 2022 for sending 498,179 unsolicited service messages about the U.K. government's "Fix Your Bike" voucher scheme, as these messages contained promotional content about Halfords Limited's services.

Guidance on Direct Marketing Using Electronic Mail

Under PECR, the general rule is that direct marketing messages can only be sent to individuals (including sole traders and some types of partnerships) by electronic mail if (1) the individual consents, or (2) the requirements of "soft opt-in" are satisfied. These rules on consent and soft opt-in do not apply to corporate entities (*e.g.*, limited liability companies and most partnerships).

The guidance covers five key principles for direct marketing using electronic mail: consent, soft opt-in, content of electronic mail, third-party marketing list and viral marketing.

Consent

The guidance provides clarity on how consent should be obtained and managed, in particular:

- **Freely given:** Individuals must be able to refuse to give consent to such electronic mail direct marketing messages without any detriment to them, and the consent request must be separated from other aspects such as the organization's terms and conditions or a new promotion.
- **Specific and informed:** Organizations must specify the particular type of electronic mail covered in the consent request (*e.g.*, email, text), allowing separate consent for each type, and provide the organization's name.
- **Unambiguous intention:** Organizations must be certain that recipients are consenting to receiving such messages.
- **Clear affirmative action:** Organizations must not rely on pre-ticked opt-in boxes, silence or inactivity to infer consent.
- **Consent is not transferrable:** Where an individual consents to receiving direct marketing messages to a particular email address or phone number, the organization cannot contact that individual at another email address or phone number for direct marketing purposes.

We have seen the ICO take enforcement action against organizations that fail to comply with these strict consent requirements. In April 2022, the ICO fined a financial services company £60,000 for sending over 500,000 unsolicited direct

marketing messages via email and text without obtaining valid consent. Specifically, the ICO noted that the consent was not (1) informed, as individuals were not notified during the finance application process that marketing messages would be sent, (2) specific, as there was no indication as to the types of marketing communication that would be sent (*i.e.*, email and text), or (3) freely given, as consent was required as a condition of making a finance application.

While it is not mandatory, the guidance recommends that organizations maintain a record of consent (*e.g.*, in the form of a suppression list that is maintained and kept up-to-date). This record may be audited by the ICO in the context of an investigation and will evidence the consent provided by individuals. For example, in September 2021, the ICO fined a sports apparel website £70,000 after it was unable to retrieve the distribution list (and associated valid consents) used to send over 2.5 million direct marketing emails. Maintaining a record of consent also is key to ensuring that organizations will cease to send such messages whenever an individual withdraws their consent. For example, in May 2021, the ICO fined a credit card company £90,000 for sending more than 4 million marketing emails (that were incorrectly categorized as service messages) to individuals who had opted out of receiving such emails.

The guidance clarifies that organizations are only required to cease sending direct marketing messages from the particular marketing method from which the consumer opts out (*e.g.*, email, text), as opposed to all methods (unless the customer opts out of all methods). Additionally, the guidance notes that organizations should cease sending direct marketing messages "as soon as possible" (as opposed to immediately), while also noting that organizations should maintain a suppression list and add an individual who withdraws their consent to such list as soon as they withdraw their consent. Additionally, the guidance notes that organizations should consider using a third-party tool or platform that allows them to track customer consent (as the consent is provided and withdrawn) in real time and to automatically add customers to a suppression list once they withdraw their consent.

Soft Opt-In

Under the soft opt-in rule, organizations are not required to obtain a customer's or prospective customer's consent to send electronic mail marketing where:

- the organization obtains the individual's contact details in the course of the sale, or negotiation for the sale, of one of its products or services;
- the marketing message relates to similar products and services to those that the individual purchased or negotiated the sale of; or
- the individual is given a simple way to opt out of receiving direct marketing messages at the point where the organization first collected their details and in every subsequent message the organization sends to the individual (*e.g.*, a clearly visible "unsubscribe" button in an email).

The guidance provides some clarity on the criteria for soft opt-in, noting:

- soft opt-in is only available to the organization that originally collects the contact details (it does not apply to other companies within the same group);
- negotiations for a sale require an individual to "actively express an interest" in buying the organization's products or services, which may include requesting a quote, asking for more details of what the organization offers or signing up for a free trial of the organization's products or services (but does not include logging into an organization's website to browse its products or submitting a general query);
- whether a product or service is "similar" is fact-specific and depends on whether the individual would reasonably expect direct marketing messages about the products or services in question (*e.g.*, a customer that buys bread from a supermarket may expect an email about other groceries sold by the supermarket, but not about unconnected services such as banking or insurance); and
- the opt-out options must be clear, simple and free of charge (*e.g.*, individuals should not be required to log in to their existing account to change their preferences).

Satisfying *all* of these requirements will be under the ICO's scrutiny. For instance, in September 2022, the ICO imposed a £200,000 fine on a car buying company for sending 191.4 million marketing emails and 3.6 million marketing text messages to individuals without, among other things, offering individuals an opportunity to opt-out of direct marketing emails at the point when the company first collected the individuals' contact details.

Content of Electronic Mail Marketing Messages

Direct marketing messages sent via electronic mail must not disguise the organization's identity and must provide a valid contact address to opt-out of such messages. These rules apply regardless of whether the recipient is an individual or a company, and regardless of whether the message is solicited.

Third-Party Marketing Lists

The guidance recognizes that organizations may purchase and/or use marketing lists compiled by third parties. While this alone would not be a breach of PECR, organizations must satisfy

that the individuals on such third-party marketing lists have consented to receiving marketing messages (1) from the organization (as opposed to the third party), and (2) via the relevant marketing channel (*e.g.*, email, text, direct message on social media). The guidance sets out a series of questions for organizations to consider to determine whether the individuals on such third-party marketing lists have provided valid consent, namely:

- What were people told?
- What did they consent to?
- Were you named on the consent request?
- When and how did they consent?
- Did they have a choice to consent?
- Is there a record of the consent?

The guidance emphasizes that the organization (as the electronic mail "sender") remains liable for any breach of PECR as a result of using such third-party marketing lists for direct marketing purposes via electronic mail.

Viral Marketing

Viral marketing refers to circumstances where an organization asks individuals to send the organization's direct marketing messages to their friends and family (*e.g.*, encouraging family and friends to sign up to the organization's product or service offering). The guidance advises organizations against creating pre-populated messages for individuals to forward to friends or families, or from actively encouraging individuals to forward direct marketing messages to their friends or families. In particular, as organizations cannot, in these instances, demonstrate valid consent from the individuals to whom such messages are sent (as they are not in direct contact with those individuals). However, the guidance notes that organizations may still offer a "refer a friend" program (*e.g.*, where an organization provides a customer with a unique discount code for referrals without telling the customer how they should make such referrals).

These principles would equally apply to a situation where one organization asks another organization to send direct marketing messages to individuals on its behalf. For example, the ICO fined a personal finance company £75,000 in September 2021 for asking two other companies to send direct marketing messages on behalf of the company. In its monetary penalty notice, the ICO noted that the company created the content of the direct marketing emails and relied on "indirect consent" (*i.e.*, the consent obtained by the other companies from the individuals concerned).

Key Takeaways

The publication of the guidance provides welcome clarity to organizations on some of the key rules on direct marketing via electronic mail, but also is an indication of the ICO's increased focus on compliance with such rules.

The guidance notes that the ICO takes a "risk-based, effective and proportionate approach" to enforcement action for noncompliance, which may include an enforcement notice requiring an organization to stop sending infringing direct marketing messages and/or a fine of up to £500,000. Recent ICO enforcement actions suggest that compliance with direct marketing rules is an enforcement priority for the supervisory authority. In the year to date, the ICO has issued 21 fines for breaches of PECR totaling more than £1.7 million. While the individual fines do not tend to reach the upper limit of £500,000 (with fines for 2022 ranging from £2,000 to £230,000), organizations may suffer additional damage from a finding of noncompliance by the ICO, including reputational damage and loss of sales.

Organizations also should be mindful that customers are increasingly aware of, and are increasingly exercising, their rights under applicable data protection laws, as ICO investigations are frequently instigated by complaints from customers. As such, organizations should familiarize themselves with the guidance to ensure their marketing policies, practices and procedures are compliant, and update them where necessary.

Return to Table of Contents

Contacts

Stuart D. Levi
Partner / New York
212.735.2750
stuart.levi@skadden.com

James Carroll
Partner / Boston
617.573.4801
james.carroll@skadden.com

Brian Duwe
Partner / Chicago
312.407.0816
brian.duwe@skadden.com

David Eisman
Partner / Los Angeles
213.687.5010
david.eisman@skadden.com

Patrick Fitzgerald
Partner / Chicago
312.407.0508
patrick.fitzgerald@skadden.com

Todd E. Freed
Partner / New York
212.735.3714
todd.freed@skadden.com

Marc S. Gerber
Partner / Washington, D.C.
202.371.7233
marc.gerber@skadden.com

Rich Grossman
Partner / New York
212.735.2116
richard.grossman@skadden.com

Ken D. Kumayama
Partner / Palo Alto
650.470.4553
ken.kumayama@skadden.com

Michael E. Leiter
Partner / Washington, D.C.
202.371.7540
michael.leiter@skadden.com

William Ridgway
Partner / Chicago
312.407.0449
william.ridgway@skadden.com

Jason D. Russell
Partner / Los Angeles
213.687.5328
jason.russell@skadden.com

David Schwartz
Partner / New York
212.735.2473
david.schwartz@skadden.com

Ingrid Vandenborre
Partner / Brussels
32.2.639.0336
ingrid.vandenborre@skadden.com

Helena Derbyshire
Of Counsel / London
44.20.7519.7086
helena.derbyshire@skadden.com

Peter Luneau
Counsel / New York
212.735.2917
peter.luneau@skadden.com

James S. Talbot
Counsel / New York
212.735.4133
james.talbot@skadden.com

Eve-Christie Vermynck
Counsel / London
44.20.7519.7097
eve-christie.vermynck@skadden.com

This communication is provided by Skadden, Arps, Slate, Meagher & Flom LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This communication is considered advertising under applicable state laws.

Skadden, Arps, Slate, Meagher & Flom LLP
One Manhattan West
New York, NY 10001
212.735.3000