February 2019

Skadden

Privacy & Cybersecurity Update

Equifax Investor Lawsuit to Move Forward

On January 28, 2019, the U.S. District Court for the Northern District of Georgia ruled that Equifax investors can sue the company and its former CEO for boasting about its cybersecurity program after consultants had uncovered flaws in the company's digital defenses.

In mid-2017, hackers stole the personally identifiable information, including Social Security numbers and addresses, of more than 148 million people by exploiting a vulnerability in software used by credit bureau Equifax. This breach gave rise to multiple litigations, including one brought by investors who purchased Equifax securities between February 2016 and September 2017.

The investors claim that Equifax, and its former CEO Richard Smith,[1] committed fraud by disseminating multiple false or misleading statements emphasizing the company's supposedly strong cybersecurity through Equifax's website, security filings and communications with investors. According to the complaint, Equifax made these statements after a third-party cybersecurity firm's audit of Equifax's systems had found that Equifax's digital defenses were "grossly inadequate," with unpatched software flaws and poor password policies. Judge Thomas Thrash emphasized that the discrepancy between the company's public statements and its knowledge of the actual state of its cybersecurity practices contributed to his decision allowing the case to move forward.

The judge stated that Equifax's specific representation that it employed a "rigorous" enterprise risk management program was more misleading than simply stating that it uses an enterprise risk management program. He also disagreed with Equifax's argument that its disclosures were "vague, meaningless statements of corporate optimism that no reasonable shareholder would rely upon in making investment decisions," noting that the importance of data security in Equifax's business means investors would be more likely to consider such representations to be important.

[1] The suit also named as defendants three other executives, who were dismissed for lack of evidence that they had any specific information about the company's cybersecurity deficiencies.

Key Takeaways

This ruling is a reminder that plaintiffs may seek to rely on a company's public statements regarding the strength of its cybersecurity program in the event of a data breach. Companies should be cautious when making these public statements and implement measures to ensure that such statements are reviewed internally by both legal and information security experts to avoid making overly optimistic or misleading claims.

Return to Table of Contents

CareFirst Data Breach Class Action Largely Dismissed

The U.S. District Court for the District of Columbia largely dismissed the *Attias v. CareFirst* data breach class action on the grounds that the plaintiffs failed to allege actual injury, as required for nine of their claims. The dismissal signifies that, while a data breach plaintiff may allege sufficient injury for standing purposes to open the courthouse doors, such injury may not be sufficient to prevent dismissal when actual injury is a requirement of the asserted claims.

Background

In 2014, CareFirst suffered a data breach in which CareFirst policyholders' names, dates of birth, email addresses, subscriber identification numbers and social security numbers allegedly were stolen. In June 2015, seven named plaintiffs brought suit against CareFirst on behalf of the 1.1 million policyholders that were potentially impacted by the data breach. On behalf of the putative class, the plaintiffs brought claims for negligence, breach of contract, breach of confidentiality, and violations of various state consumer protection and data breach notification statutes, among others. The district court dismissed on Article III standing grounds, explaining that, "[a]bsent facts demonstrating a substantial risk that stolen data has been or will be misused in a harmful manner, merely having one's personal information stolen in a data breach is insufficient to establish standing to sue the entity from whom the information was taken." Key to the district court's determination was that only two members of the putative class alleged actual identity theft.

The D.C. Circuit reversed, holding that policyholders had "cleared the low bar to establish their standing at the pleading stage" by asserting a "substantial risk" that their stolen personal information could be used "for ill" purposes, such as identity theft, in the future. Thereafter, the U.S. Supreme Court denied CareFirst's petition for *certiorari*, in which CareFirst argued that, for standing purposes, a plaintiff must not only allege a "substantial risk that a future injury will occur" but also that the alleged injury is "imminent." Injury was not imminent, according to CareFirst, because the plaintiffs had "not suffered any identity theft or other harm in the more than three years since the breach." In denying *certiorari*, the Supreme Court declined to resolve the circuit split on whether a plaintiff may establish Article III injury-in-fact based on a mere increased risk of future identity theft.

The District Court Decision

Upon remand from the D.C. Circuit, and more than 1,400 days after the data breach, CareFirst renewed its motion to dismiss. The district court granted the motion, "in large part," because, "while plaintiffs' alleged injuries may be enough to establish standing at the pleading stage of the case, they are largely insufficient to satisfy the 'actual damages' element of nine of their state-law claims."

Among the plaintiffs' alleged injuries were "(1) actual and/or heightened risk of misuse of personal information, (2) loss of the 'benefit of the bargain' they struck when they purchased their policies, [and] (3) consequential damages like expenditures [on] credit monitoring services."

As for the first theory, that the data breach subjected plaintiffs to "actual or heightened risk of misuse of exposed personal information," the court concluded that "only two of the named plaintiffs" actually "allege that they have already experienced any kind of economic injury." This was fatal to the plaintiffs' negligence and breach of confidentiality claims under District of Columbia law because a binding D.C. Court of Appeals' decision "declined to treat an increased risk of future identity theft as an actual harm for [those] claims."

The court then concluded that the plaintiffs' "benefit-of-the-bargain" theory was too "indeterminate" to establish actual injury, because plaintiffs did not allege that a portion of their health insurance premiums went toward providing data security. Citing Article III cases where courts found the "benefit-of-the-bargain" theory insufficient to establish injury-in-fact, the court explained that "the standard for alleging actual damages is generally higher than that for plausibly alleging injury-in-fact."

The plaintiffs also argued that they "have or will spend significant time and money to protect themselves" after the data breach, such as by purchasing identity theft protection and better data monitoring services. Courts have distinguished between expenditures incurred in response to identity theft and those incurred to prevent it, with the latter not constituting "actual damages" because they are not premised on an actual injury of identity theft. Rather, they are premised on an "anticipated" injury, albeit one that may suffice to establish injury for Article III standing purposes.

Key Takeaways

Even if a plaintiff can allege injury-in-fact sufficient for Article III standing purposes, that injury may not be enough to survive dismissal. As *CareFirst* shows, the same injury arguments found lacking for dismissal on standing grounds may suffice for dismissal on the merits if the asserted claim contains "actual injury" as an element, particularly when years have passed since the data breach. For data breach plaintiffs who bring suit immediately after a breach and before any injury materializes, Article III standing is therefore only the first obstacle they will need to overcome.

Return to Table of Contents

President Launches Federal AI Initiative

President Donald Trump signed an executive order on February 11, 2019, titled "Maintaining American Leadership in Artificial Intelligence,"[2] which directs certain federal agencies to prioritize research and development of artificial intelligence (AI) and assist with the development of technological standards to support reliable, robust and trustworthy AI systems.

The executive order designates the National Science and Technology Council Select Committee on Artificial Intelligence to coordinate a federal initiative to promote AI development based on five guiding principles:

1. The U.S. must drive technological breakthroughs in AI across the federal government, industry and academia in order to promote scientific discovery, economic competitiveness and national security.
2. The U.S. must drive development of appropriate technical standards and reduce barriers to the safe testing and deployment of AI technologies in order to enable the creation of new AI-related industries and the adoption of AI by today's industries.
3. The U.S. must train current and future generations of American workers with the skills to develop and apply AI technologies to prepare them for today's economy and jobs of the future.
4. The U.S. must foster public trust and confidence in AI technologies and protect civil liberties, privacy and American values in their application.
5. The U.S. must promote an international environment that supports American AI research and innovation, and opens markets for American AI industries, while protecting the country's technological advantage in AI and protecting critical AI technologies from acquisition by strategic competitors and adversarial nations.

The executive order also directs agencies that conduct foundational AI research and development, develop and deploy AI applications, provide educational grants, and regulate and provide guidance for the development of AI applications to pursue six strategic objectives to promote and protect American advancements in AI:

1. Promote sustained investment in AI research and development in collaboration with industry, academia, international partners and allies to generate technological breakthroughs in AI.
2. Enhance access to high-quality and fully traceable federal data, models and computing resources to increase the value of such resources for AI research and development, while maintaining safety, security, privacy and confidentiality protections consistent with applicable laws and policies.
3. Reduce barriers to the use of AI technologies to promote their innovative application while protecting American technology, economic and national security, civil liberties, privacy and values.
4. Ensure that technical standards minimize vulnerability to attacks from malicious actors and reflect federal priorities for innovation, public trust and public confidence in systems that use AI technologies.

[2] The full text of the executive order is available here.

5. Train the next generation of American AI researchers and users through apprenticeships; skills programs; and education in science, technology, engineering and mathematics.
6. Develop and implement an action plan to protect the advantage of the United States in AI and technology critical to United States economic and national security interests against strategic competitors and foreign adversaries.

The executive order does not identify any new funding sources to support its strategic objectives. However, it directs certain federal agencies to prioritize research and development in AI when developing budget proposals and planning for the use of funds in upcoming years. Under the executive order, all federal agencies must identify opportunities to increase access and use of federal data and models by the greater AI research community while protecting privacy, security and safety. Recognizing that federal agencies may not be in the best position to identify the data sets or models that private sector and academic researchers may find useful, the executive order also mandates the publication of a notice in the Federal Register to invite the public to request access or quality improvements in federal data and models that would improve research, development and funding of AI.

The executive order also requires the directors of the Office of Management and Budget, Office of Science Technology and Policy, Domestic Policy Council and National Economic Council to issue a memorandum to the heads of all federal agencies to guide the development of regulatory and non-regulatory approaches to advance AI. Beyond the development of initial regulatory guidance, the executive order also directs the National Institute of Standards and Technology (NIST) to issue a plan for federal engagement in the development of technical standards and related tools to support reliable, robust and trustworthy AI systems. The executive order requires NIST to consult with the private sector, academia and other stakeholders regarding the development of such technical standards.

Key Takeaways

The executive order recognizes the need for a coordinated approach at the federal level to promote the responsible development of AI. Instead of relying on a top-down regulatory approach, the executive order encourages input from the private sector, academia and federal agencies with experience in AI development. Companies for which AI plays a strategic role should monitor these developments and consider participating in opportunities to collaborate with the federal government on these initiatives.

Return to Table of Contents

US Government Accountability Office Report Recommends Federal Data Privacy Legislation

On February 13, 2019, the U.S. Government Accountability Office (GAO) publicly released its report, "Internet Privacy: Additional Federal Authority Could Enhance Consumer Protection and Provide Flexibility" (GAO Report), advising Congress on developing comprehensive privacy legislation.

In the wake of several incidents involving the disclosure of personal consumer information of millions of Americans, the GAO was asked to review and report on federal oversight of internet privacy. The purpose of the GAO Report is to evaluate (1) how the Federal Trade Commission (FTC) and Federal Communications Commission (FCC) oversee consumers' internet privacy, (2) selected stakeholders' views on the strengths and limitations of current federal internet privacy oversight and how it could be improved, and (3) the benefits and concerns associated with the collection of internet users' personal information for commercial purposes.[3] To conduct its research, the GAO interviewed representatives from industry stakeholders from a range of different sectors, consumer advocacy groups and academics; FTC and FCC staff; former FTC and FCC commissioners; and officials from other federal oversight agencies.

Stakeholders interviewed by the GAO had wide-ranging views on the current approach to internet privacy enforcement. Industry stakeholders (including internet service providers from different sectors, *i.e.*, cable, satellite and telephone-based services, and internet content providers that provide a variety of information and social media services) indicated that the FTC has been effective and favorably viewed the FTC's current approach of direct enforcement. These stakeholders expressed concerns regarding the promulgation of regulations for several reasons, including the potential for regulations to stifle innovation, to contain loopholes susceptible to exploitation, to quickly become obsolete in the rapidly changing internet industry and to be too time-consuming to implement.

In contrast, the majority of non-industry stakeholders (including all former FTC commissioners that were interviewed, three of the four former FCC commissioners that were interviewed and the consumer advocacy group representatives) identified shortcomings in the current internet privacy oversight framework. These stakeholders had a more favorable view of regulations and took

[3] Full report available here.

the position that regulations in conjunction with enforcement were more likely to be effective. They noted that regulations can clarify expectations for companies, promote fairness by creating a consistent regime, provide flexibility by targeting behaviors rather than specific technologies and deter bad practices in the industry. In addition, they noted that the enforcement-only approach is limited in its *post hoc* nature, in contrast to regulations, which could encourage desirable behavior *ad hoc*.

Stakeholders identified three main avenues through which internet privacy oversight could be enhanced:

- the implementation of an overarching federal internet privacy statute to establish general requirements governing privacy practices across all sectors that effectively could articulate to consumers, industry and privacy enforcers which behaviors are prohibited and which are encouraged, and create a consistent standard that has the goal of consumer protection as a guiding principle;
- the use of Administrative Procedure Act Section 553 "notice-and-comment" rulemaking authority in order to promulgate rules; and
- enhancement of the FTC's ability to levy civil penalties for initial violations and to impose larger civil penalties, which stakeholders believe could be particularly effective in industries where there is little competition and thus more opportunity to pass the cost of the fines along to consumers.

Key Takeaways

Following the enactment of the EU General Data Protection Regulation (GDPR), the California Consumer Protection Act and the string of recent security and data breaches involving the disclosure of personal data of millions of Americans, pressure from consumer advocates for more robust privacy protection has been mounting. The GAO Report considers the viewpoints of advocates for and against further federal oversight of internet privacy and recommends that Congress should consider developing comprehensive privacy legislation to strengthen consumer protections. It remains to be seen whether Congress will follow these recommendations.

Return to Table of Contents

Three State Legislatures Adopt Variations of NAIC Insurance Data Security Model Law

The South Carolina, Ohio and Michigan legislatures have adopted variations of the National Association of Insurance Commissioners' (NAIC) Insurance Data Security Model Law (Model Law). These state law enactments are a step toward establishing more uniform standards for data security and breach notification in the domestic insurance industry.

Three states — South Carolina, Michigan and Ohio — recently adopted the NAIC Model Law,[4] which establishes minimum data security standards and obligations applicable to a broad range of insurance industry participants, including insurers, brokers and producers. South Carolina enacted its version of the NAIC Model Law in May 2018, while both Michigan and Ohio adopted variations in December 2018. The South Carolina law went into effect January 1, 2019; Ohio goes into effect on March 20, 2019; Michigan goes into effect January 20, 2021.

Comparison of the State Laws With the NAIC Model Law

These state enactments are similar to the NAIC Model Law in a number of respects. For example, the NAIC Model Law and the state laws broadly define "nonpublic information" to include personal information as well as "business-related" information that, if compromised, would result in a "materially adverse impact" to the business, operation or security of a "licensee," which is defined to include insurers, agents, brokers and other persons and entities required to be licensed under state law.

Additionally, the state laws, like the NAIC Model Law, require licensees to perform comprehensive risk assessments to identify reasonably foreseeable threats that could result in unauthorized access, transmission, disclosure, misuse, alteration or destruction of nonpublic information and assess those threats based on their likelihood and potential damage, as well as the adequacy of safeguards in place. As with the NAIC Model Law, the three state laws also require licensees to "develop, implement, and maintain a comprehensive written information security program, based on

[4] See our October 2017 *Privacy & Cybersecurity Update* for a discussion of the NAIC Model Law, available here.

the licensee's risk assessment." Under the state law enactments, licensees also are required to exercise diligence in selecting third-party service providers and to demonstrate appropriate oversight of any such third parties.

With respect to data breaches, as with the NAIC Model Law, the state laws require covered entities that suffer a data breach to notify their respective state insurance regulator if either South Carolina, Ohio or Michigan is the insurer's state of domicile or if the event affects 250 or more consumers residing in the state. In addition, all three state laws require that licensees provide material updates to the state insurance regulator during the organization's investigation of the breach, as does the NAIC Model Law. However, the state law breach notification deadlines vary. South Carolina requires licensees to notify the state insurance regulator within 72 hours of detection of a cybersecurity event; Ohio provides licensees with three business days to notify the state superintendent of a cybersecurity event; Michigan allows licensees 10 business days to report a cybersecurity event to the state insurance director.

Under the NAIC Model Law, licensees with fewer than 10 employees are exempt from the law's information security program requirements, but not the notice and investigation requirements. The Michigan and Ohio laws are similar in this respect in that they also exempt small businesses from information security program requirements required by their respective laws. However, Michigan's law provides the exemption to licensees with fewer than 25 employees, while Ohio's law provides the exemption to licensees with fewer than 20 employees or with less than either $5 million in gross annual revenue or less than $10 million in total assets at the conclusion of the licensee's fiscal year. South Carolina, by contrast, entirely exempts licensees with fewer than 10 employees from compliance with its law.

Finally, unlike the NAIC Model Law, Ohio's statute contains a "safe harbor" provision that provides licensees that comply with the law an affirmative defense against tort claims alleging that the licensee failed to implement reasonable cybersecurity controls. Notably, the "safe harbor" serves as a defense only against causes of action brought under Ohio law.

Key Takeaways

State law variations in data security and breach notification requirements continue to place substantial costs and burdens on the insurance industry. These three states' recent enactments of permutations of the NAIC Model Law may encourage other states to follow suit. While any move toward greater uniformity is welcome, material variations persist, requiring insurance industry participants to remain vigilant regarding state law distinctions.

Return to Table of Contents

New York's Department of Financial Services Publishes Guidance on Use of Non-Traditional External Data

The New York Department of Financial Services (DFS) recently released a memorandum formally approving and providing guidance regarding the use of "unconventional sources or types of external data" in underwriting and setting premiums for life insurance.

On January 18, 2019, the DFS became the first state insurance regulator to formally approve and provide guidance on the use of external consumer data, such as social media and other non-traditional sources, in life insurance underwriting and pricing. The DFS' guidance, which is directed to all insurers authorized to write life insurance in New York state, is set forth in Insurance Circular Letter No. 1 (Circular).[5]

Impetus for the DFS Guidance

Following reports of an increased use of unconventional sources of external data in the insurance underwriting process, the DFS launched an investigation into life insurers' underwriting guidelines and practices in New York related to the use of such data. As explained in the Circular, "external data" refers to data sources not directly related to the medial condition of the applicant that are used to supplement traditional medical underwriting — either as a proxy for traditional underwriting or to establish lifestyle indicators that contribute to the underwriting assessment.

The Circular acknowledges that there are a number of potential benefits to using external data in the underwriting process. For example, the Circular points out that the use of predictive models, algorithms and related technology may improve access to financial services, simplify and expedite life insurance sales and underwriting, and increase the accuracy and pricing of life insurance.

[5] Insurance Circular Letter No. 1, Use of External Consumer Data and Information Sources in Underwriting for Life Insurance (Jan. 18, 2019), available here.

At the same time, however, the Circular acknowledges that the use of external data also has the potential to negatively impact consumers, insurers and New York's life insurance marketplace. According to the Circular, the DFS has "two particular areas of immediate concern with the use of external data sources." The first concern is unlawful discrimination: The use of external data sources may have a significant negative impact on the availability and affordability of life insurance for protected classes of consumers. The second concern is transparency: The use of external data "is often accompanied by a lack of transparency for consumers." The Circular provides guidance with respect to these two key concerns.

Guidelines on Preventing Unlawful Discrimination

To address the DFS' concerns with respect to potential unlawful discrimination, the Circular provides two principles for insurers to use as guidance in utilizing external data sources. First, an insurer using an external data source, algorithm or predictive model in underwriting or rating must independently confirm that the external tools or data sources do not collect or utilize prohibited criteria (race, color, creed, national origin, status as a victim of domestic violence, past lawful travel, sexual orientation or any other protected class). The Circular emphasizes that an insurer may not simply rely on a vendor's claim of non-discrimination or the proprietary nature of a third-party process as justifications for the failure to independently vet the external tools or data sources. Second, an insurer should not use an external data source, algorithm or predictive model in underwriting or rating unless the insurer can establish that the underwriting or rating guidelines "are not unfairly discriminatory" in violation of New York's insurance laws.

Guidelines on Promoting Transparency

The Circular similarly provides guidance with respect to the transparency concern. It explains that under New York law, insurers are required to notify the insured of the right to know the specific reason(s) for a declination, limitation, rate differential or other adverse underwriting decision. The Circular states that where an insurer uses an external data source, algorithm or predictive model, the reason(s) provided to the insured "must include details about all information … including the specific source of the information" on which the insurer based its decision. As in the unlawful discrimination context, an insurer may not rely on the proprietary nature of a third-party vendor's algorithmic processes to justify the lack of specificity related to an adverse underwriting decision.

Key Takeaways

The DFS guidance is the first of its kind in the U.S. However, in light of the growing use of external data in underwriting and concerns over the application of such data, other state insurance regulators may be inclined to follow suit. Moreover, while there certainly may be practical challenges to implementing the Circular's guidance, on balance, the guidance set forth in the Circular may help promote predictability and stability in the life insurance marketplace.

Return to Table of Contents

Germany's Federal Cartel Office Restricts Facebook from Combining User Data From Different Sources

On February 6, 2019, Germany's Federal Cartel Office (FCO) issued a decision prohibiting Facebook Inc., and its subsidiaries Facebook Ireland Ltd. and Facebook Germany GmbH (together, Facebook), from making users' access to its social network conditional on the collection of user data from multiple sources without the user's consent. While the FCO did not impose fines on Facebook, it restricted the way Facebook can collect and process user data from multiple sources, including Facebook-owned services such as Instagram or WhatsApp.

Background

Under Facebook's terms and conditions, a user can use facebook.com only if Facebook can collect and combine a user's data from multiple sources, including Facebook-owned services such as WhatsApp and Instagram, and third-party websites and smartphone apps that include interfaces, such as the Facebook "Like" or "Share" buttons, or that use the Facebook Analytics service in the background.

The FCO determined that Facebook's collection and combining of user data from various sources without the user's consent violates European data protection provisions and also could be prohibited as an "exploitative abuse" under German competition law rules.

Decision

The FCO held that Facebook holds a dominant position in a German market for social networks, referring to Facebook's high share of daily and monthly active users. The FCO noted that services like Snapchat, YouTube or Twitter, as well as professional networks like LinkedIn and Xing "only offer parts of the services of a social network" and would therefore not be included in the relevant market.

The FCO concluded that the extent to which Facebook collects, merges and uses data in user accounts constitutes an abuse of its dominant position. The FCO clarified that it does not take issue with the way Facebook processes data generated by the use of Facebook's own website, as such data collection constitutes "an essential component of a social network and its data-based business model." However, the FCO determined that Facebook's terms and conditions allow it to collect an "almost unlimited amount" of user data from Facebook-owned services and third-party sources. The FCO referenced third-party sources that are visible to the user, such as the "Like" or "Share" buttons that collect data even if the user does not scroll over or click on the button, and data sourcing that is invisible to the user such as the use of the Facebook Analytics service in the background of third-party websites.

In the FCO's view, Facebook's terms and conditions, and the manner and extent to which it collects and uses data, are in violation of the European data protection rules and constitute "inappropriate contractual terms and conditions," which in turn constitute an "exploitative abuse" of a dominant position under German competition rules. In a press release, the FCO's president remarked in this context that "[t]oday data are a decisive factor in competition. In the case of Facebook they are the essential factor for establishing the company's dominant position. … It is therefore precisely in the area of data collection and data use where Facebook, as a dominant company, must comply with the rules and laws applicable in Germany and Europe."

In its decision, the FCO imposed the following restrictions on Facebook:

- Facebook-owned services such as WhatsApp and Instagram can continue to collect data but may only link the data to a Facebook user account with the user's consent.
- Collecting data from third-party websites and smartphone apps, and linking such data to a Facebook user account, also will only be permitted with the user's consent.
- If users do not consent, Facebook cannot exclude them from its services. Facebook has four months to submit proposals for possible solutions to comply with these requirements and 12 months to adjust its terms and conditions, as well as its data and cookie policies.

The FCO's decision is not yet final, and Facebook has one month to appeal the decision to the Düsseldorf Higher Regional Court.

Key Takeaways

The FCO's decision is a landmark ruling that has attracted significant international interest. It is a novel ruling in that it constitutes the first decision in which a competition authority has based its finding of an abuse of a dominant position under competition law on a violation of data protection and privacy rules. The European Commission, which has closely monitored the FCO's investigation, explained after the publication of the FCO's decision that EU data protection law (the GDPR that entered into force in May 2018) "addresses this type of conduct," which suggests that the European Commission may not bring a competition case on the basis of a data protection or privacy law violation, at least in the short term. However, it remains to be seen whether national competition regulators, in the EU or elsewhere, feel encouraged by the FCO's decision to initiate competition law investigations for data protection violations. In parallel, data protection authorities remain competent to pursue data protection law violations, including in the EU, on the basis of the GDPR.

Return to Table of Contents

Privacy & Cybersecurity Update
Update

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
213.687.5381
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

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

Amy Park
Partner / Palo Alto
650.470.4511
amy.park@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

Ivan Schlager
Partner / Washington, D.C.
202.371.7810
ivan.schlager@skadden.com

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

Jen Spaziano
Partner / Washington, D.C.
202.371.7872
jen.spaziano@skadden.com

Donald L. Vieira
Partner / Washington, D.C.
202.371.7124
donald.vieira@skadden.com

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

Jessica N. Cohen
Counsel / New York
212.735.2793
jessica.cohen@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

Ingrid Vandenborre
Partner / Brussels
32.2.639.0336
ingrid.vandenborre@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
Four Times Square
New York, NY 10036
212.735.3000