Skadden

Privacy & Cybersecurity Update

All 50 States Now Have Data Breach Notification Laws

South Dakota and Alabama became the final two states to pass data breach laws, with both laws mirroring previous laws that have been passed in other states around the country.

In March 2018, Alabama and South Dakota enacted data breach notification requirements, meaning that all 50 states now have such a law.

South Dakota

The South Dakota data breach law (SB 62[1]) defines personal information as an individual's first name or first initial and last name, in combination with any of the following: Social Security number; driver's license number or other government-issued unique identification number; credit or debit card number if combined with the required security code, access code, password, routing number, PIN or any other information that might allow access to a person's financial account; or any employee ID if combined with a required security code, access code, password or biometric data.

Notice is required within 60 days, however, as in a number of states, there is an exception if the information holder determined, following "an appropriate investigation and notice to the attorney general," that the breach will not likely result in harm to the affected persons.

Notice to the state's attorney general is required if the breach involves more than 250 South Dakota residents, with notice to the nationwide consumer reporting agencies always required.

Interestingly, a violation of the law is deemed a "deceptive act" under South Dakota consumer protection laws, meaning that a private right of action may exist if the law is violated. The South Dakota law will take effect on July 1, 2018.

[1] The text of the law can be found here.

Alabama

The Alabama law (SB 318[2]) requires notification within 45 days, and also requires data processors who handle personal information to notify the covered entity within 10 days. Notice to the Alabama attorney general and consumer reporting agencies is required if more than 1,000 individuals have been affected by the breach.

Personal information is defined similarly to the South Dakota law, but also includes any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; an individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual; and/or a user name or email address, in combination with a password or security question and answer, that would permit access to an online account affiliated with the covered entity that is reasonably likely to contain, or is used to obtain, personally identifying information.

Notice is not required if the covered entity determines after reasonable analysis that the breach is not likely to cause substantial harm to the individuals to whom the information relates.

As with South Dakota, the Alabama attorney general may prosecute a failure to disclose a data breach as an unlawful act or practice under the Alabama Deceptive Trade Practices Act.

The law also imposes a number of security obligations, including: identification of internal and external risks of a breach of security; designation of an employee to coordinate the covered entity's security measures to protect against a breach of security; and keeping the management of the covered entity, including its board of directors, if any, appropriately informed of the overall status of its security measures.

Key Takeaways

The passage of both of these states' laws means that all 50 states now have data breach notification laws.

Return to Table of Contents

[2] The text of the law can be found here.

State Attorneys General Push Back Against Federal Data Breach Notification Law

State attorneys general have begun to argue against a federal data breach notification law in response to the recently introduced Data Acquisition and Technology Accountability and Security Act, with more than half of the states stating their opposition in a letter to congressional committee. Thirty-one state attorneys general have opposed a recently introduced federal data breach notification law arguing that states should be able to impose their own individual requirements.

Any company that has suffered a data breach is all too aware of the fact that data breach notification requirements are imposed at the state law level. With the passage of laws by Alabama and South Dakota (see above article in this *Update*), a company must now comply with 50 state laws if it suffers a nationwide data breach. While it would be erroneous to say there are 50 different laws since many states have mirrored the laws of others, there is enough variation to create headaches for any company seeking to comply with these notification requirements.

As a result, there has been an understandable push for a federal omnibus data breach notification law, such as the recently introduced Data Acquisition and Technology Accountability and Security Act. Companies might therefore be surprised that this act actually has been opposed by 31 attorneys general, including those from California, Illinois and Massachusetts. In a letter to members of the Financial Services Committee, the attorneys general argue that states are more nimble at revising laws as technology and cyberattacks change compared to federal regulators and should therefore have jurisdiction over these matters. State attorneys general voiced a similar view in 2005 when it seemed like a federal law was a possibility. The attorneys general also noted that while national breaches get the most attention, many are at a state or regional level, showing the states should therefore not be pre-empted from dictating the required notice.

The attorneys general also were critical of the act's requirement that breach notification only be required if a company believes there is a reasonable risk of identity theft, economic loss or fraud. In the view of these states, notification should be required in all instances.

Return to Table of Contents

FBI Director Calls for Greater Public-Private Partnership to Fight Cyber Threats

The director of the Federal Bureau of Investigation (FBI) declared his support for an increase in cooperation between his agency and the private sector regarding cybersecurity, wading into a controversial debate among companies over whether to provide data to federal and local intelligence and law enforcement agencies.

At a cybersecurity conference in Boston in early March 2018, FBI Director Christopher Wray called for increased partnership between the FBI and the private sector to face the growing threat of cyberattacks.

Wray emphasized the importance of data protection in the FBI's mission in light of both the increasing complexity of potential targets and the increasing sophistication of threats in the cybersecurity landscape — including the increase in nation-state-sponsored cyberattacks, such as recent, costly attacks attributed to North Korea (WannaCry) and Russia (NotPetya).

Acknowledging "we know we can't prevent every attack, or punish every hacker," Wray argued that improved cybersecurity requires strengthened partnerships among federal law enforcement agencies, international partners and corporate stakeholders.

Importantly, Wray emphasized that public-private partnerships must be two-way streets to be effective. While he called on organizations to notify the FBI when they find indications or evidence of cyberattacks, such as malware or significant losses of data, Wray acknowledged that the agency is working to better communicate indicators of compromise, tactics of attackers and strategic threat information to private sector partners. Wray's comments echoed earlier statements from FBI leadership, such as the February 2018 remarks by FBI Deputy Assistant Director Howard Marshall, who explained that "the FBI is enhancing the way it communicates with private industry" and looking to "integrate private industry information into [its] intelligence cycle."

Perhaps most significantly, Wray noted that in furtherance of the agency's desire to partner with the private sector, the FBI will "treat victim companies as victims" and that their focus will be on doing everything they can to help them. This approach to cyber incidents is an important consideration for companies, as historically cyber victims have been subjected to regulatory scrutiny following disclosures of data breaches or other cybersecurity incidents. For example, companies often balance disclosure of actual or suspected cyberattacks with the threat of fines, lawsuits, investigations and consent order requirements from regulators such as the Federal Trade Commission and state attorneys general. Wray's statement regarding treating victim companies as victims rather than wrongdoers may, if effectively coordinated on a practical and policy level with regulators, incentivize faster and more detailed disclosures to the FBI.

Wray also reiterated that encryption of devices and communications is one of the agency's biggest challenges and requires increased engagement from the private sector. He explained that the "FBI supports information security measures, including strong encryption … [b]ut information security programs need to be thoughtfully designed so they don't undermine the lawful tools we need to keep the American people safe." He urged the private sector to innovate and develop mechanisms to allow companies to respond to court orders in a lawful way while still fostering strong cybersecurity practices. Wray also fought back against the contention that law enforcement wants "backdoors" into systems, explaining that law enforcement only wants "the ability to access [a] device" once it has obtained a lawful warrant. Wray provided the example of banks agreeing with the New York Department of Financial Services to maintain copies of encrypted communications for seven years and providing copies of the encryption keys to independent custodians as one creative way the private sector has effectively addressed this compromise.

Key Takeaways

While Wray's statements are a helpful reminder about the potential benefits of information-sharing and coordination with law enforcement when facing cyberattacks, their operational impact is still to be determined. Many security regulators do not appear to share the view that companies experiencing a data breach are victims, but rather continue to view them as examples of a lack, or failure, of security controls. The debate over device encryption and providing law enforcement access to users' information also continues. As such, companies still face difficult decisions and must weigh multiple important factors when deciding if and how to partner with law enforcement on cybersecurity issues.

Return to Table of Contents

Second Circuit to Consider Whether Computer Fraud Coverage Extends to Losses Resulting From Email 'Spoofing' Scams

The U.S. Court of Appeals for the Second Circuit is poised to rule on the issue of whether computer fraud insurance coverage extends beyond traditional direct hacking incidents to cover losses resulting from email "spoofing" scams, a growing source of cybercrime.

An appeal by Federal Insurance Company (Federal) is currently pending before the Second Circuit stemming from a Southern District of New York decision,[3] which held that one of Federal's insured clients, Medidata Solutions, Inc. (Medidata), a cloud-based services provider, is entitled to coverage under its computer fraud policy for a $4.8 million loss sustained as a result of an email "spoofing" scam that tricked Medidata into wiring the money overseas. With the rapid rise in cybercrime, multiple courts throughout the country have similarly been faced with determining whether computer fraud coverage extends beyond traditional hacking incidents to reach social engineering loss, but have thus far reached conflicting decisions. The Second Circuit's decision will be instructive and may change policyholders and insurers' perspectives on insuring against cybercrime.

The Email 'Spoofing' Incident and Medidata's Insurance Claim

In September 2014, an employee in Medidata's accounts payable department received an email from a fraudster posing as the company's president explaining that Medidata was close to finalizing an acquisition, and that an attorney copied on the email (in fact another fraudster) would be contacting the employee for assistance with the transaction. The email appeared to be legitimate — it contained the president's email address, name and picture — and after engaging in telephone and email communications with the fake attorney and receiving approval from legitimate Medidata officers, the accounts payable employee wired $4.8 million into a Chinese bank account controlled by the fraudsters. Medidata did not discover the fraud until after the funds were transferred, and the funds were never recovered.

Medidata filed a claim under its "Executive Protection" policy issued by Federal, which provided coverage for a variety of risks including "direct loss[es]" suffered by Medidata as a result of "computer fraud," which was defined to include "fraudulent entry" or changing of data in the insured's computer system. After Federal denied coverage, Medidata filed the instant coverage action.

The Southern District of New York Finds Coverage

On the parties' motions for summary judgment, the court sided with Medidata. In holding that Medidata's loss was covered under the policy's "computer fraud" coverage, the court relied on a decision by the New York Court of Appeals in *Universal American Corp. v. National Union Fire Insurance Co. of Pittsburgh, Pa.*,[4] which interpreted the phrase "fraudulent entry" of data, as used in a computer fraud policy, as a "violation of the integrity of the computer system through deceitful and dishonest access." Adopting a broad reading of *Universal*, the court held that "the fraud on Medidata falls within the kind of 'deceitful and dishonest access' imagined by the New York Court of Appeals" because the fraudster used a computer code to alter a series of emails to make them appear as though they originated from Medidata's president.

In so holding, the court rejected Federal's argument that the *Universal* ruling should be interpreted as limiting the "fraudulent entry" of data to situations where the fraudsters hack directly into a company's computer system, reasoning that hacking was "one of the many methods" that a fraudster can employ to defraud an insured. The fraudster's use of email "spoofing" to scam Medidata is a form of "fraudulent entry" that falls within the scope of the computer fraud provision, according to the court. "[L]arceny by trick is still larceny," the court noted. The court likewise rejected Federal's argument that there was no "direct nexus" between the fraudulent emails and the transfer, pointing out that the Medidata employee sent the money as a direct result of the fraudster's emails.

Federal's Appeal to the Second Circuit

On appeal to the Second Circuit, Federal argued that the district court's decision was "a serious outlier," citing the "multiple" decisions that have denied coverage for similar losses. In Federal's view, the district court improperly interpreted *Universal* by concluding that Medidata's loss was the type of unauthorized "deceitful and dishonest" access envisioned by the ruling. Federal argued that the social engineering scam was not covered by the computer fraud provision because it did not involve a "fraudulent entry" into Medidata's computer system or a "fraudulent change" to its data elements required to trigger the provision. Instead, the "spoofed" emails were created on the fraudster's computer before being sent to Medidata and were sent to an email address that accepts emails sent by outsiders. Medidata also argued that the computer fraud provision did not apply because the emails were not the direct cause of the wire transfer. Rather, the emails were merely part of the "lengthy chain of other intervening actions" that needed to occur before the transfer was authorized and executed, Federal argued.

[3] *Medidata Solutions, Inc. v. Federal Ins. Co.*, 268 F. Supp. 3d 471 (S.D.N.Y. 2017).

[4] 25 N.Y.3d 675 (2015).

In its appellate brief filed late last month, Medidata urged the Second Circuit to affirm the district court's ruling, arguing that the "spoofing" scam was precisely the type of deceitful and dishonest act contemplated by *Universal*. According to Medidata, "[w]hat matters under the policy language, as construed by the New York Court of Appeals, is whether the code contained in the emails violated the integrity of Medidata's computer system through deceitful and dishonest access. And the fraudster's manipulation of the email code, which was directed at the computer system itself, did just that." Countering Federal's causation argument, Medidata argued that the emails directly caused the loss because they were the "crucial elements" of the fraud that induced the employee to transfer the funds.

Key Takeaways

The Second Circuit's decision may turn on how it reads *Universal*. It could distinguish the *Universal* ruling based on the language of the computer fraud provision in Federal's policy. However, if the court finds the policy in *Universal* similar to the policy here, the court will have to decide whether to read Universal narrowly so as to limit coverage to direct hacking incidents, or broadly so as to extend coverage to more attenuated social engineering schemes. The Second Circuit's decision will be instructive and may change the calculus for both policyholders and insurers on how to cover cybercrime. Regardless of the outcome, this case serves as an important reminder to insurers and insureds alike to clearly set forth the terms and conditions of cyber coverage when agreeing to the policy.

Return to Table of Contents

Ninth Circuit Reaffirms Future Risk of Harm Meets *Spokeo*'s Standing Requirements in Data Breach Cases, Deepening Circuit Divide

The Ninth Circuit's decision to reverse a district court's case furthered the differing opinions at the circuit level over the degree of harm claimants must show in cyber breach cases.

On March 8, 2018, a Ninth Circuit panel reversed the district court's dismissal of plaintiffs' claims for lack of standing in a consolidated action arising from a data breach, holding that the plaintiffs sufficiently alleged an injury based on future risk of identity fraud and theft.[5] In doing so, the court reaffirmed its previous decision in *Krottner v. Starbucks*[6] and deepened the circuit split over the nature of the harm plaintiffs must allege to satisfy the standing requirements for data breach cases established in *Spokeo Inc. v. Robins*[7].

Background

The lawsuit in *In re Zappos.com, Inc., Customer Data Security Breach Litigation* arose after hackers breached the database of online retailer Zappos, accessing personal identifying information (PII) of over 24 million customers, including names, full credit and debit card information, account numbers, passwords, email addresses, billing addresses, shipping addresses and telephone numbers. On January 16, 2012, Zappos alerted its customers to the breach in an email and recommended they reset both their Zappos account passwords and similar passwords used for other websites.

Customers began filing putative class actions against Zappos that same day. Some plaintiffs alleged they suffered actual financial losses from the breach, while others alleged they were injured solely because the breach created an elevated risk of identity theft and fraud. The district court dismissed the latter group's claims for lack of Article III standing, finding those plaintiffs failed to allege "actual" identity theft or fraud.

The Ninth Circuit's Decision

On appeal, a unanimous three-judge panel reversed the District Court's denial of standing, reaffirming that future risk of identity theft or fraud is sufficient for Article III standing in data breach cases.

The court cited its 2010 decision in *Krottner v. Starbucks*, where a laptop containing unencrypted personal information, including Social Security numbers, of Starbucks employees had been stolen. Though the only harm most plaintiffs alleged was an "increased risk of future identity theft," based on the sensitivity of the compromised personal information the *Krottner* court determined that this was sufficient for Article III standing because the plaintiffs had "alleged a credible threat of real and immediate harm."

As in *Krottner*, the sensitivity of the information compromised in the Zappos hack rendered the risk of future identity theft sufficiently substantial to justify standing. The court noted that Zappos "effectively acknowledged" that the stolen information "gave

[5] *Stevens v. Zappos.com., Inc.*, No. 3:12-cv-00325-RCJ-VPC, (Ninth Cir. 2018).

[6] 628 F.3d 1139 (9th Cir. 2010).

[7] 136 S.Ct. 1540 (2016).

hackers the means to commit fraud or identity theft" when it urged affected customers to change their passwords. Additionally, the fact that a number of related plaintiffs alleged that they had already suffered identity fraud, commandeered accounts and financial losses "undermine[d] Zappos's assertion that the data stolen in the breach [could not] be used for fraud or identity theft."

The Ninth Circuit also addressed how its decision was not inconsistent with the Supreme Court's 2013 decision in *Clapper v. Amnesty International USA*.[8] In Clapper, the plaintiffs challenged surveillance procedures authorized by the Foreign Intelligence Surveillance Act of 1978 and argued they had standing because there was "an objectively reasonable likelihood that their communications would be acquired under" the statute. The Supreme Court disagreed, holding that because the plaintiffs' theory of harm depended on a "multi-chain of inferences," the injury alleged was too remote to establish standing. The Supreme Court held that to establish standing, the alleged injury must be "certainly impending" or indicative of a "substantial risk" of harm.

Krottner and *Zappos* were distinguishable from *Clapper*, the Ninth Circuit determined, because the alleged future harm did not depend on a similar chain of multiple inferences. Rather, the data breach itself created a "substantial risk" of harm.

Circuits Remain Split

The Ninth Circuit's decision in *Zappos* deepens the current circuit split on the question of whether the risk of future identity theft and fraud is alone sufficient to establish Article III standing in data breach cases. The Ninth, Sixth and Seventh Circuits have all held that it is. However, the Second, Fourth and Eighth Circuits have held that future risk of identity theft and fraud is too remote of an injury to satisfy standing. In February 2018, the Supreme Court declined to address the issue, denying *certiorari* in *CareFirst, Inc. v. Attias*.[9]

In *Zappos*, the Ninth Circuit distinguished cases from both the Eighth and Fourth Circuits based on factual differences, noting that the standing questions in data breach cases ultimately turn on the details of the breach presented in each case, particularly the sensitivity of the data stolen. Until the Supreme Court addresses the issue, courts may veer towards a fact-dependent analysis of standing.

Key Takeaways

The risk of future harm as a basis for standing remains viable in many circuits, and the cases tend to depend on the circumstances of the breach and the sensitivity of the data compromised. Moreover, companies dealing with a data breach must be careful not to inadvertently acknowledge the risk of future fraud and identity theft in its external communications.

Return to Table of Contents

FTC Identifies Mobile Security Update Inconsistency as Key Industry Risk

The Federal Trade Commission (FTC) released a commission report that highlights the uncertain state of mobile security today due to manufacturers creating or modifying different operating systems to suit their devices' needs.

In February 2018, the FTC released a commission report that highlights the uncertain state of mobile security. Because the mobile device industry has an array of manufacturers, each of which are creating or modifying different operating systems to suit their devices' needs, the response time to any security threat can differ. In light of this fragmentation in the industry — including differences in hardware and operating systems, as well the varying popularity of particular devices — the FTC report analyzes manufacturers' security update practices, offering recommendations to improve the efficacy and responsiveness of the security update process.[10]

Characteristics of Some Industry Participants

The FTC noted that within the mobile device industry, many manufacturers customize their third-party operating system software at the device level. This means that operating system updates to patch security holes may require hundreds of device-level modifications. These differences, combined with necessary testing by the manufacturers and carriers before the update is deployed, can result in a significant delay between the time a security risk is identified and its patch is released. Adding to the variability of an update schedule is the fact that many manufacturers prefer "just-in-time" support, basing their decisions on a device's popularity

[8] 568 US 398 (2013).

[9] 583 U.S. __ (February 20, 2018).

[10] The FTC's report is available here.

and age, the cost of support, partner input, the severity of the vulnerability and timing of regularly scheduled releases. Furthermore, while some manufacturers make update support information available to consumers before purchase, many manufacturers do not maintain regular update support records at all. Additionally, while some manufacturers have been proactive in streamlining their security processes, the FTC believes the current paradigm leaves much room for improvement.

Benefits and Risks

While diversity in the industry has given consumers more choice, it also has led to fragmentation between devices that contributes to security update inconsistency since uniform security patches cannot be developed. Furthermore, with increased diversity among product lines, manufacturers are unlikely to support the device with security updates for long periods of time, instead tending to focus support updates on their newest or more expensive models. Finally, while carrier testing adds another level of assurance that the update is stable, it also adds to what are already typically lengthy delays.

Recommendations

The FTC has issued five recommendations to improve security update consistency and efficacy:

- government, industry and advocacy groups should work together to educate consumers about the significance of security updates and the role the consumer plays in them;
- the mobile device industry should embed security support considerations into design and support culture and decisions from the beginning stages of a device's conception;
- the mobile device industry should consider maintaining records about support length, update decisions, frequency and consumer acceptance so the industry can develop best practices;
- the mobile device industry should streamline the update process by creating faster security-only updates that are not bundled with general software updates; and
- manufacturers should consider guaranteeing minimum support periods and frequencies for their devices and notifying consumers when support will end.

Key Takeaways

The recommendations provided by the FTC aim to build upon the improvements to which the mobile device industry has already committed, with the aim of making security updates a primary consideration for consumers choosing a device.

Return to Table of Contents

UK Proposes New Security Measures for Consumer Internet of Things

On March 7, 2018, a British government agency released a rigorous new proposal requiring makers of internet-connected devices to take certain measures to protect users of these devices from cybersecurity threats.

Secure by Design Report

The U.K. Department for Digital, Culture, Media & Sport issued a report on improving the cybersecurity of consumer internet of things (IoT) devices, proposing a range of measures to better protect users of these products. The report notes that smart devices, such as televisions and toys linked to the expanding IoT space, provide significant technological advancements for consumers as well as the U.K.'s digital economy. However, many of these devices lack even basic cybersecurity measures, leaving consumers vulnerable to data privacy and security risks.[11]

The "Secure by Design" report notes that in order to adequately protect consumers from these risks, the burden must shift from end-users (consumers) to the makers of these products. Rather than expecting consumers to securely use and configure their IoT devices, strong security must be built into these devices by design. The report's primary recommendation requires IoT device-makers to build in resilient security measures that last for the lifetime of the product during the design process, rather than tacking them on as an afterthought. The report outlines a code of conduct that requires IoT devices to encrypt sensitive transmitted data and maintain timely software updates, prohibits the use of default passwords and ensures manufacturers of IoT devices have a vulnerability policy in place.

[11] The full report is available here.

The report also proposes developing a product labeling scheme, akin to a nutrition label, that would provide information to make consumers aware of a product's security features at the point of purchase.

The agency teamed up with expert advisory groups and subject-matter leaders from the industry in developing its recommendations. The report is part of the U.K.'s major effort to become an international leader in the development and upkeep of the IoT. The plan is open to public comment through April 25, 2018.

Implications for IoT Device Manufacturers in the US

The FTC deems itself a watchdog for U.S. consumers' privacy in the IoT, and has, in the past, filed complaints against IoT device manufacturers for poor security measures.[12]

[12] For more, see our February 2018 *Privacy & Cybersecurity Update* here.

In addition to the U.K. proposals, companies can adopt the FTC best practices, including:

- building security into devices at the outset, rather than as an afterthought, in the design process;
- when a security risk is identified, considering a "defense-in-depth" strategy whereby multiple layers of security may be used to defend against a particular risk; and
- considering measures to keep unauthorized users from accessing a consumer's device, data or personal information stored on the network.

Key Takeaways

The U.K. agency's report signifies an increased worldwide focus on the safety and security of IoT devices. The report promotes, among other ideas, significant thought to design changes, both in the design and maintenance of devices to protect security of data and personal information.

Return to Table of Contents

Contacts in the Cybersecurity and Privacy Group

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

Lisa Gilford
Partner / Los Angeles
213.687.5130
lisa.gilford@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

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

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

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

Skadden, Arps, Slate, Meagher & Flom LLP
Four Times Square
New York, NY 10036
212.735.3000