Skadden

Privacy & Cybersecurity Update

1 Ohio Statute Creates Affirmative Defense for Data Breach Claims

2 Federal Judges Scrutinize Class Actions in Data Breach Cases

3 California Enacts Law to Strengthen Internet-of-Things Security

4 California Passes Amendments to Its Newly Enacted Omnibus Privacy Law

5 Data Breach Reports Significantly Increase in the UK Under the GDPR

6 Appeals Courts Reject Calls to Reconsider Decisions That Computer Fraud Insurance Coverage Extends to Social Engineering Losses

Ohio Statute Creates Affirmative Defense for Data Breach Claims

Ohio has provided a safe harbor from tort-based data breach claims if the company adopts certain security measures before a breach occurs.

Ohio recently enacted a new statute — the Ohio Data Protection Act — which creates an affirmative defense against tort claims arising out of a data breach.[1] The affirmative defense under the statute, which goes into effect on November 2, 2018, can be asserted only by entities that have adopted a written cybersecurity program in line with the statute's requirements. Unlike Massachusetts, which requires entities that own or license personal information of its residents to maintain a written information security program, Ohio has opted to incentivize — but not require — companies to create and maintain such a program and improve their data security practices. Ohio is the first state to provide companies with such a safe harbor.

How to Benefit From the Affirmative Defense

The law creates an affirmative defense from tort-based data breach claims for covered entities, defined as businesses that access, maintain, communicate or process personal information or restricted information in or through one or more systems, networks or services located in or outside Ohio. Covered entities can assert this new affirmative defense once they create, maintain and comply with a written cybersecurity program that contains administrative, technical and physical safeguards for the protection of personal information and restricted information, and that reasonably conforms to at least one industry-recognized cybersecurity framework from a list set forth in the statute. That list includes the commonly followed NIST Framework for Improving Critical Infrastructure Cybersecurity and ISO/IEC 27001.

Personal information is defined as an individual's name in combination with a Social Security number, driver's license number or state identification card number, or account number or credit or debit card number, in combination with and linked to any required security code, access code or password where the data elements are not encrypted or otherwise unreadable. Restricted information is defined as any information about

[1] The full text of the Ohio Data Protection Act.

an individual other than personal information that, alone or in combination with other information — including personal information — can be used to distinguish or trace the individual's identity, or is linked or linkable to an individual, if the information is not encrypted or otherwise unreadable and its breach is likely to result in a material risk of identity theft or other fraud to that person or property.

The program must be designed to do the following:

- Protect the security and confidentiality of the information;
- Protect against any anticipated threats or hazards to the security or integrity of the information; and
- Protect against unauthorized access to and acquisition of the information that is likely to result in a material risk of identity theft or other fraud to the individual to whom the information relates.

Ohio has recognized that written information security programs may differ depending on the size of the covered entity and the nature of the personal information processed by the entity. The Ohio Data Protection Act provides that the scale and scope of a covered entity's cybersecurity program is "appropriate" if it is based on the following factors:

- The size and complexity of the covered entity;
- The nature and scope of the activities of the covered entity;
- The sensitivity of the information to be protected;
- The cost and availability of tools to improve information security and reduce vulnerabilities; and
- The resources available to the covered entity.

Importantly, the statute does not protect against all potential claims or fines arising out a data breach. The statute also does not prevent individuals from filing tort-based claims in response to a data breach. Instead, the statute entitles covered entities to an affirmative defense from any tort-based causes of action that allege that the failure to implement reasonable information security controls resulted in a data breach concerning personal information.

Key Takeaways

Ohio is the first state in the nation to create an affirmative defense against tort-based data breach claims for companies that meet certain data security standards. Companies will no doubt appreciate the opportunity to limit their data breach liability with respect to such claims, even as their potential liability for contract-based claims and governmental fines continues to rise. Whether other states follow Ohio's lead remains to be seen.

Return to Table of Contents

Federal Judges Scrutinize Class Actions in Data Breach Cases

Courts in two data breach class action cases recently rejected global settlements proposed by the parties based on concerns about intraclass conflicts, settlement recoveries and attorneys' fees. Both of these rulings reflect a recent trend of heightened judicial scrutiny of settlements in data breach class actions.

The Neiman Marcus Class Action

After Neiman Marcus suffered a major data breach that compromised customers' credit card information in 2013, multiple class actions against the company were consolidated in the U.S. District Court for the Northern District of Illinois. In 2016, the assigned judge preliminarily certified a proposed class that included consumers who shopped at Neiman Marcus between the date of the data breach and the date of its disclosure to the public. That judge later retired, however, and the case was reassigned. On September 17, 2018, the new judge assigned to the case denied the plaintiffs' motion to approve the settlement and for attorneys' fees, and decertified the settlement class.[2]

In doing so, the court heeded warnings issued by the U.S. Court of Appeals for the Eighth Circuit in 2017 in *In re Target Corp. Customer Data Security Breach Litigation*, which instructed courts to consider: "whether an intraclass conflict exists when class members who cannot claim money from a settlement fund are represented by class members who can."[3] The court divided the affected Neiman Marcus customers into three subgroups: (1) consumers whose credit card information was exposed and abused when the malware was active; (2) consumers whose credit card information was exposed but not abused when the malware was active; and (3) consumers who did not face credit card exposure because they made purchases between the end of the breach and its disclosure to the public. The court found that an intraclass conflict existed for the third subgroup because, unlike the first two subgroups, members in that subgroup had no reason to base a settlement recovery on credit card exposure or fraud.

According to the court, a conflict did not exist between the first two subgroups because the class representatives had equal incentive to represent both groups. The incentives aligned because the settlement agreement prevented class members from knowing whether their information had been compromised until after

[2] *Remijas et al v. The Neiman Marcus Group, LLC*, No. 14-01735 (N.D.I.L. Sept. 17, 2018).

[3] *In re Target Corp. Customer Data Sec. Breach Litig.*, 847 F.3d 608 (8th Cir. Feb. 1, 2017).

they opted into the settlement. The court noted, however, that if any named plaintiff had discovered this information, intraclass conflicts could exist between the first two subgroups as well.

In response to the data breach, Neiman Marcus also offered class members a year of free credit monitoring and identity theft insurance, and enhanced the company's cybersecurity business practices. The court indicated that these activities could not constitute nonmonetary relief because they had been offered prior to any settlement, and the company's business practices were nonbinding.

The Kimpton Class Action

In 2016, Kimpton, a luxury brand that owns boutique hotels and restaurants, announced a data breach that compromised customer information. A class action was filed soon thereafter in the U.S. District Court for the Northern District of California. On September 13, 2018, the court denied a motion for preliminary approval of a settlement agreement based on concerns about the settlement recovery and attorneys' fees.[4] The court ruled that $15 per hour for time spent protecting against identity theft was too low and that a three-hour cap on the number of recoverable hours was unreasonable. The court also held that $800,000 in attorneys' fees and Kimpton's promise to not challenge the request was "unjustified" due to the $600,000 cap on the settlement recovery and the expected low participation rate in the settlement.

Key Takeaways

These cases reflect the growing trend signaling courts are closely scrutinizing intraclass conflicts, settlement recoveries and attorneys' fees in data breach class actions. Such scrutiny may pose a challenge to litigants seeking settlements in data breach cases, particularly where the settlement involves a large class of customers. Companies also should be mindful that any relief offered presettlement, such as credit monitoring and identity theft insurance, cannot later be cited as a nonmonetary benefit in a settlement and should be aware that attorneys' fees must bear a relationship to the recovery for class members.

Return to Table of Contents

[4] *Parsons v. Kimpton Hotel & Restaurants Group, LLC*, No. 16-05387 (N.D.C.A. Sept. 13, 2018).

California Enacts Law to Strengthen Internet-of-Things Security

California has enacted a law requiring internet-of-things (IoT) device manufacturers to implement certain security features starting in 2020.

California has enacted a law (SB-327) mandating "reasonable" security features for IoT devices, which include smart watches, smart speakers and smart appliances.[5] These devices connect to the internet in order to gather data from, or transmit data to, servers and provide the user its "smart" features. For example, a user can use her smartphone to turn on or adjust a WiFi-enabled lightbulb in her house without the use of a physical switch.

Many security experts have cautioned that, to date, IoT devices have generally not been developed with security as a top priority. While most IoT devices do not have the processing power of a typical computer, they function similarly in that they have processors and are able to connect to the internet. Unlike a typical computer, however, most IoT devices cannot be patched to run firmware updates to improve the device's security and therefore are prime targets for hackers. On October 21, 2016, for example, the "Mirai" botnet was able to compromise vulnerable IoT devices simply by using a roster of 61 username/password combinations that are frequently used as factory-setting default credentials. With the combined processing power of these many compromised IoT devices, the Mirai botnet launched a massive distributed denial-of-service (DDoS) attack that shut down the internet for much of the United States' East Coast for nearly 12 hours. Furthermore, IoT devices not only pose cybersecurity risks, they also can pose privacy risks. The ubiquitous data collection of certain IoT devices can leave a "digital residue," which, when pieced together, can reveal a near-complete profile of the device's user. This customer data could then be sold to third parties.[6]

California is attempting to address the risk of such IoT-based attacks, among other potential issues, with Senate Bill 327. The bill requires that, beginning on January 1, 2020, IoT device manufacturers must equip their devices with "a reasonable

[5] The full text of SB-327 is available here.

[6] See Skadden's January 2015 *Privacy and Cybersecurity Update* for a summary of the dangers of unsecured IoT devices.

security feature or features that are appropriate to the nature and function of the device, appropriate to the information it may collect, contain, or transmit, and designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure." One such manifestation of this requirement is that the device's password is either preprogrammed to be unique to each device manufactured or designed to require the user to generate a new means of authentication before the user can access the device. Though many experts agree that Senate Bill 327 is a step in the right direction because it recognizes the risks that unprotected IoT devices pose, some critics argue that it will do little to improve security and will stifle innovation.

Key Takeaways

As a leader in both privacy and cybersecurity considerations in the United States, with the passage of the California Consumer Privacy Act in June 2018 and now Senate Bill 327, California hopes that other states, as well as the federal government, will take similar steps in order to regulate an industry that has thus far been largely unregulated. Other nations, such as the United Kingdom, have taken similar steps to regulate the IoT industry, demonstrating the growing urgency with which the world is grappling with these issues.[7] As the data privacy and cybersecurity problems surrounding IoT devices continue, we may see laws similar to California's Senate Bill 327 in the future.

Return to Table of Contents

California Passes Amendments to Its Newly Enacted Omnibus Privacy Law

The California Legislature has passed an amendment to the California Consumer Privacy Act (CCPA) that includes extending the date by which the state attorney general must adopt implementing regulations.

In the final hours of the 2018 legislative session, the California Legislature passed SB-1121,[8] an amendment to the CCPA, which was enacted on June 28, 2018. As we previously noted in our July 11, 2018, client alert, the CCPA is by far the broadest and most comprehensive privacy law enacted in the United States to date.

The amendment, which has been approved by the governor, corrects a number of drafting errors in the hastily passed CCPA legislation, and also includes certain substantive revisions. The key amendments are summarized below with our observations in italics:

- **An Extension of the Deadline for Finalization of Regulations and Enforcement Actions.** SB-1121 delays the requirement for California's attorney general to adopt implementing regulations for the CCPA from January 1, 2020, to July 1, 2020. Enforcement actions may not be brought by the attorney general under the CCPA until the earlier of July 1, 2020, or six months after the publication of final regulations. *Given the haste with which the CCPA was passed, many had expressed concern over the short time period to come into compliance. While January 1, 2020, is over a year away, many companies have seen how long it took to comply with the European General Data Protection Regulation (GDPR). This extension and delay in enforcement will be welcomed by all companies who need to comply with the CCPA.*
- **Narrowing Private Right of Action.** SB-1121 clarifies that the CCPA's private right of action applies only to certain limited data security events and does not apply to other violations of the CCPA, including its privacy obligations. *This amendment clarifies concerns that the CCPA would dramatically expand private rights of action.*
- **Elimination of AG "Gatekeeping" Function for Private Right of Action.** SB-1121 eliminates the CCPA's requirement that consumers provide the California attorney general with 30 days of notice prior to filing a private suit under the CCPA to allow the attorney general to object to the suit. *While this requirement seemed to provide a check on private rights of action, it was unclear how it would have been implemented in practice prior to its elimination.*
- **Clarification and Expansion of the GLBA and DPPA Exceptions.** The CCPA exempts "personal information collected, processed, sold or disclosed pursuant to the federal Gramm-Leach-Bliley Act (Public Act 106-102) [(GLBA)], and implementing regulations" and the Driver's Privacy Protection Act of 1994 (DPPA) if the CCPA is in conflict with GLBA or the DPPA. SB-1121 removes the "in conflict with" requirement, thereby exempting any data processed pursuant to the GLBA and DPPA. In addition, SB-1121 expands the exemption to apply to information collected, processed, sold or disclosed pursuant to the California Financial Information Privacy Act (CFIPA). Note, however, that consumers will still have a private right of action with respect to data security events involving information subject to the GLBA, DPPA or

[7] See Skadden's March 2018 *Privacy and Cybersecurity Update* for a summary of the U.K.'s IoT report.

[8] The full text of SB-1121 is available here.

CFIPA because the exceptions do not apply with respect to CCPA's private right of action. *The initial draft of the CCPA created considerable confusion because of its "in conflict with" provision. Removal of this provision and expansion to include the CFIPA are therefore important changes.*

- **Expansion of the HIPAA Exception and New Clinical Trial Exception.** The CCPA exempts medical information either under California's Confidentiality of Medical Information Act (CMIA) or collected by a covered entity under the Health Insurance Portability and Accountability Act (HIPAA). SB-1121 expands the scope of this exception to health information covered under HIPAA collected by a "business associate" of a covered entity. SB-1121 also exempts health care providers (governed by CMIA) or covered entities (governed by HIPAA) to the extent that such entities maintain information in the same manner as medical information subject to CMIA or protected health information subject to HIPAA. Additionally, SB-1121 adds a new exception from CCPA for information collected as part of a clinical trial subject to guidelines issued by the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use or the U.S. Food and Drug Administration. *The expansion of the health information exemption clarifies ambiguity that existed under the initial draft of the CCPA.*
- **Clarification of Civil Penalties.** SB-1121 clarifies that businesses that violate the CCPA may be subject to an injunction and statutory damages of either $2,500 per each nonintentional violation or $7,500 per each intentional violation.

Key Takeaways

Although SB-1121 provides some important clarifications to the CCPA, many provisions of the CCPA remain ambiguous (including, for example, the status of anonymized information and clarification regarding how businesses can satisfy *ex ante* notice requirements with respect to the collection and use of personal information). Given the remaining ambiguities, it is likely that there will be another effort to amend the CCPA in the 2019 legislative session.

Return to Table of Contents

Data Breach Reports Significantly Increase in the UK Under the GDPR

The number of data breaches reported to data protection authorities has dramatically increased in the United Kingdom since the implementation of the GDPR, though the increase does not necessarily suggest a rise in the number of data breaches.

The European Union's GDPR, which went into effect on May 25, 2018, as supplemented in the U.K. by the Data Protection Act 2018, requires controllers to notify the applicable data protection authority of personal data breaches without undue delay. Additionally, where feasible, the authority must be notified no later than 72 hours after becoming aware of the breach either internally or through an external processor, unless the breach is unlikely to result in a risk to the affected individuals' rights and freedoms.[9] Although the GDPR refers to a "high risk" threshold to determine whether notification to affected data subjects themselves is required,[10] the GDPR does not similarly qualify the "risk" that triggers the notification requirements to a supervisory authority. This ambiguity has led some controllers to err on the side of caution in the early months of this new legal framework, resulting in some overreporting, as reflected in initial data released by several supervisory authorities.

Increase in Reports to Data Protection Authorities

The United Kingdom's Information Commissioner's Office (ICO) received 1,792 reports of personal data breaches in June 2018, compared to only 657 reports in May 2018.[11] ICO Deputy Commissioner (Operations) James Dipple-Johnstone recently commented[12] on this increase, as the ICO has been receiving around 500 calls a week to its breach reporting line since May 25, 2018. About one in five reported breaches involve cyber incidents, nearly half of which are the result of phishing. By way of comparison, the ICO received 398 data breach reports in March

[9] GDPR Article 33.

[10] GDPR Article 34.

[11] The ICO discussed these figures during a recent webinar.

[12] James Dipple-Johnstone's speech to the CBI Cyber Security: Business Insight Conference.

2018 and 367 data breach reports in April 2018. Similarly, *The Irish Times* recently reported that Ireland's Data Protection Commission received more than 1,100 data breach reports in a two-month period after the implementation of the GDPR.[13] On average, the Irish Data Protection Commission had received 230 data breach reports per month in the previous year.[14]

The number of data protection-related complaints filed with the relevant supervisory authorities also has increased since the implementation of the GDPR. France's data protection authority, the Commission Nationale de l'Informatique et des Libertés, recently reported that it had received 1,804 complaints between May 25, 2018, and July 31, 2018, a significant increase compared to the 1,132 complaints received during the same time period last year.

Evidence of 'Overreporting'

Although data protection-related complaints have risen along with reports of personal data breaches, data protection authorities have suggested that at least some of the increase in data breach reports can be attributed to overreporting. Many controllers are likely concerned with failing to report within the 72-hour time frame — and having to pay the resulting administrative fines — and are therefore reporting personal data breaches even when those breaches do not necessarily meet the reporting threshold. Controllers also may be unsure of what breaches qualify as reportable under the GDPR.

Laura Middleton, who leads the ICO's personal data breach enforcement team, emphasized during the ICO's recent webinar on data breach reporting that data controllers should take the time to determine whether a breach is actually reportable under the GDPR's requirements before notifying the applicable supervisory authority. This also was highlighted by Dipple-Johnstone, who said that roughly a third of the 500 calls the ICO has received per week to its breach reporting line since May 25, 2018, are from companies that, after internal discussions, decided that their breach did not meet the reporting threshold.

On that note, the ICO has published its reporting guidance online and have set forth the approach under its Regulatory Action Policy (subject to parliamentary approval).[15] This approach is risk-based when deciding whether to take regulatory action against companies and individuals that have breached the applicable data protection provisions.

Key Takeaways

As with many provisions of the GDPR, companies find themselves in a period of uncertainty as to how the data breach reporting requirement will be interpreted by supervisory authorities. The ICO has issued specific advice to assist companies as they assess whether submitting a report is necessary, including by encouraging them to read the ICO's reporting guidance,[16] take the time to gather information internally and report by phone if companies need advice on how to manage the breach or whether or not to tell affected individuals.

As part of general cybersecurity response planning, companies should consider involving their data protection governance team from the outset to assess the seriousness of the breach and promptly take all necessary measures to mitigate a breach. Companies also should be aware of the EU directive on the security of network and information systems, also known as NIS Directive, which was implemented by the U.K.'s Network and Information Systems Regulations 2018. Those regulations mandate a 72-hour breach notification regime to the competent authorities for operators of essential services, including, without limitation, digital service providers that may be required to report to the ICO. In light of this accountability principle, companies will be required to keep a log of all personal data breaches and document their reasoning regardless of whether they ended up notifying the competent supervisory authority or not.

Return to Table of Contents

Appeals Courts Reject Calls to Reconsider Decisions That Computer Fraud Insurance Coverage Extends to Social Engineering Losses

The U.S. Courts of Appeals for the Second and Sixth circuits recently denied motions to reconsider decisions that computer fraud coverage extends to losses resulting from email spoofing scams.

On August 28, 2018, the Sixth Circuit denied reconsideration of its decision concluding that Michigan-based tool and die manufacturer American Tooling Center, Inc.'s (ATC) computer fraud insurer, Travelers Casualty and Surety Company of America (Travelers), must cover an $834,000 loss suffered after ATC employees were tricked by an email spoofing scam that caused

[13] "DPC Receives Over 1,100 Reports of Data Breaches Since Start of GDPR Rules," *The Irish Times*.

[14] "GDPR Effect: Data Protection Complaints Spike," *Bank Info Security*.

[15] The ICO Regulatory Action Policy.

[16] ICO's "Report a Breach" literature.

them to wire company money to an imposter's bank account.[17] The Sixth Circuit's decision came on the heels of the Second Circuit's August 23, 2018, decision declining to reconsider its decision similarly concluding that Medidata Solutions, Inc.'s computer fraud insurer, Federal Insurance Company (Federal), must cover a $4.8 million loss suffered after Medidata fell victim to an email spoofing scam that caused it to wire money to fraudsters overseas.[18]

The Sixth Circuit Decision

The lawsuit in the Sixth Circuit, which we previously discussed,[19] arose in 2015, when a fraudster posing as an ATC vendor emailed ATC requesting over $800,000 in legitimate outstanding invoices. When ATC sued for coverage, the U.S. District Court for the Eastern District of Michigan sided with Travelers, reasoning that the transfer of funds was not a "direct loss" — as required by the policy — because ATC verified the invoices and initiated payment without verifying bank details.

A panel of the Sixth Circuit disagreed. The court rejected the district court's narrow definition of "direct loss," concluding that ATC's wiring of money was a direct loss even though it did not know about the fraud until later. The court also rejected Traveler's argument that "computer fraud" was limited to "hacking and similar situations," holding that "computer fraud" covered ATC's money transfer prompted by the fraudster's email.

On August 28, 2018, the court summarily denied Traveler's petition for rehearing or rehearing *en banc*.

[17] *Am. Tooling Ctr., Inc. v. Travelers Cas. & Sur. Co. of Am.*, No. 17-2014 (6th Cir. Aug. 28, 2018).

[18] *Medidata Solutions., Inc. v. Fed. Ins. Co.*, No. 17-2492, 2018 WL 3339245 (2d Cir. Aug. 23, 2018).

[19] See our August 2018 and December 2017 issues of *Privacy & Cybersecurity Update*.

The Second Circuit Decision

The lawsuit in the Second Circuit, which we also have previously discussed,[20] arose in 2014 when fraudsters posing as Medidata's president and attorney emailed and called a company employee to ask for assistance with a transaction. The company employee — after receiving approval from legitimate company officers — wired $4.8 million to the fraudsters before discovering that the request was a fraud. Medidata sued Federal, claiming coverage for computer fraud, and the U.S. District Court for the Southern District of New York sided with Medidata. The court applied a broad reading of New York Court of Appeals precedent in holding that the fraudster's use of computer code qualified as a "violation of the integrity of the computer system through deceitful and dishonest access" and that the transfer was a "direct loss."

In a brief summary order, a panel of the Second Circuit agreed. The panel concluded that the policy's "plain and unambiguous" language covered the losses, reasoning that the fraudsters manipulated Medidata's email system with a computer-based attack using code that altered the system's appearance. The court rejected Federal's argument that Medidata did not suffer a "direct loss," reasoning that the chain of events "was initiated by the spoofed emails, and unfolded rapidly following their receipt."

On August 23, 2018, the court summarily denied Federal's petition for rehearing or rehearing *en banc*.

Key Takeaways

Whether this pair of decisions is unique to the policies at issue or signals a broader shift in how courts view computer fraud coverage is yet to be seen. In the meantime, policyholders, insurers and brokers alike should continue monitoring new case law addressing coverage for social engineering loss. Additionally, parties to insurance contracts should carefully review their policies to confirm that they accurately reflect the parties' understanding of the scope of coverage to be afforded.

Return to Table of Contents

[20] See our July 2018 and March 2018 issues of *Privacy & Cybersecurity Update*.

Privacy & Cybersecurity 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

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

William Ridgway
Partner / Chicago
312.407.0449
william.ridgway@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

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

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