Skadden

Privacy & Cybersecurity Update

1 Credit Union's Data Breach Suit Against Eddie Bauer Moves Forward

2 Ruling in *US v. Glassdoor* Distinguishes Ninth Circuit Precedent for Online Privacy Protection

3 United Kingdom's National Audit Office Releases Report on Effects of WannaCry Cyberattack

4 White House Details US Government's Cost-Benefit Analysis for Releasing Zero-Day Vulnerabilities

5 Surveillance Court Rules ACLU and Yale Clinic Have Standing to Pursue Release of Section 215 Rulings

6 District Court Holds That Insurer's Written Privacy Pledge to Insured is Unenforceable in Data Breach Row

7 SWIFT Report Highlights Changing Cyber Threat Landscape for Financial Institutions

Credit Union's Data Breach Suit Against Eddie Bauer Moves Forward

A Washington state court allowed a data breach lawsuit against clothing company Eddie Bauer to proceed, finding that, under Washington law, Eddie Bauer owed a duty to Veridian, a credit union, and, as a result, the company's failure to implement adequate measures to protect payment card information could constitute negligence.

Background

In August 2016, Eddie Bauer LLC (Eddie Bauer) announced that it had detected malware on cash registers at approximately 350 stores throughout the U.S. and Canada, compromising customer data from January 2, 2016, to July 17, 2016. In a complaint filed in March 2017, Veridian argued that Eddie Bauer's failure to implement appropriate security controls constituted negligence, and, as a result of such negligence, Veridian and other financial institutions incurred significant costs associated with notifying customers of the breach, reissuing customers' credit and debit cards, and refunding customers for fraudulent charges. Veridian alleged that if Eddie Bauer had followed sufficient security protocols, the data breach and subsequent costs to financial institutions like Veridian would not have occurred. Eddie Bauer moved to dismiss the lawsuit on the grounds that Veridian failed to allege sufficient facts to support its claims. On November 9, 2017, a federal judge in Washington state allowed the credit union's class action lawsuit against Eddie Bauer to proceed.[1]

Recent Ruling

Negligence

The U.S. District Court for the Western District of Washington found that Veridian's negligence claim against Eddie Bauer could move forward because Eddie Bauer owed

[1] For the full order on Eddie Bauer's motion to dismiss, see here.

Veridian a duty to safeguard its cardholders' data under Washington state law RCW 19.255.020. Under law, if a business engaged in payment processing "fails to take reasonable care to guard against unauthorized access to account information … and the failure is found to be the proximate cause of a breach, the processor or business is liable to a financial institution for reimbursement of reasonable actual costs related to the reissuance of credit cards and debit cards that are incurred to mitigate potential current or future damages to its credit card and debit card holders that reside in the state of Washington."[2] The court found that the harm specified in RCW 19.255.020 matches that alleged by Veridian in its negligence claim and, accordingly, that Eddie Bauer owed a duty to Veridian.

Washington Consumer Protection Act

The court also allowed Veridian to proceed with its claim under Washington's Consumer Protection Act (CPA). Veridian alleged that Eddie Bauer's failure to adopt reasonable security measures resulted in harm to thousands of customers and payment card issuers. Eddie Bauer argued that Veridian failed to allege unfair or deceptive practices because consumers could have avoided the risk of data theft by paying for items at the affected stores with cash. The court rejected this argument, calling it "disingenuous" given the prevalence of credit and debit card use in commerce. The court agreed with Veridian that customers could not possibly have known that Eddie Bauer's security measures were allegedly inadequate. Without this knowledge, consumers had little ability to avoid the harms brought about by Eddie Bauer's allegedly deficient security measures.

Eddie Bauer also unsuccessfully argued that a failure to enact stronger cybersecurity measures could not by itself cause harm to shoppers, but rather could only cause harm when a third party steals customer information. The court stated that Eddie Bauer's assertion distorts causation under the CPA — an "unfair act" does not need to be the most proximate cause of the alleged injury in order to give rise to liability. In this case, Eddie Bauer's alleged failure to adopt reasonable security protocols could constitute an "unfair act" within the meaning of the CPA because it knowingly and foreseeably put customers and payment card financial institutions at risk of harm from data theft and fraudulent payment card activity.

[2] For the full text of RCW, see here.

Key Takeaways

While the final outcome of the case remains to be seen, this recent ruling is interesting because of its reliance on negligence as a theory of liability between two sophisticated parties. Financial institutions and retailers alike should be aware that statutes like Washington state's may be leveraged to support negligence claims in the event of a data breach affecting payment card information.

Return to Table of Contents

Ruling in *US v. Glassdoor* Distinguishes Ninth Circuit Precedent for Online Privacy Protection

The U.S. Court of Appeals for the Ninth Circuit rejected Glassdoor's attempt to quash a subpoena seeking the identity of users of the site who had posted anonymous reviews of their employer.

Background

In connection with an ongoing federal grand jury investigation of a government contractor that administered VA health care programs, an Arizona federal grand jury had served Glassdoor — an online platform that allows employees to post anonymous reviews about their employers, including information relating to salaries, workplace environment and interview practices — with a subpoena for its users' information related to reviews of the contractor they had posted to the site. Although Glassdoor reviews are anonymous, users must provide their email address to register on glassdoor.com. As well, Glassdoor's privacy policy warns users that, if required by law, the company will "disclose data if [they] believe in good faith that such disclosure is necessary … to comply with relevant laws or to respond to subpoenas or warrants or legal process served on [them]."

The subpoena initially required Glassdoor to produce every review for the contractor, along with identifying information about the reviews' authors, such as email addresses, billing information, credit card information and other information stored on Glassdoor's platform. The company objected, citing First Amendment concerns.

When Glassdoor refused to supply the requested user-identifying information, the government limited the scope of its request, proposing instead that Glassdoor provide the user information for only eight reviews, based on the government's belief that such users were witnesses to their employer's unlawful conduct. Glassdoor again refused and filed a motion to quash the subpoena. The district court, after applying the good-faith test established by the U.S. Supreme Court in *Branzburg v. Hayes*, 408 U.S. 665 (1972), denied Glassdoor's motion and ordered the company to respond to the subpoena.

Ninth Circuit Ruling Upholds District Court Judgment

On appeal to the Ninth Circuit, Glassdoor argued that the subpoena violated its users' First Amendment rights, specifically their right to associational privacy and anonymous speech. The Ninth Circuit rejected these arguments, finding that because Glassdoor users are strangers to each other and are not joined in a common endeavor. Thus, they do not have a right to associational privacy. The Ninth Circuit further noted that the right to anonymous speech is limited and that the government's interest in investigating fraudulent activity outweighed the right to anonymous speech under these circumstances.

Although Glassdoor argued that the Ninth Circuit should apply the compelling-interest test established by the Ninth Circuit's ruling in *Bursey v. United States*, 466 F.2d 1059 (9th Cir. 1972), the court instead relied on *Branzburg*, thereby upholding the district court's ruling. Applying the *Branzburg* good-faith test, the court held that "absent a colorable allegation of bad faith on the part of the government, and without a credible argument that there is a tenuous relationship between the information Glassdoor holds and the focus of the investigation … Glassdoor's motion to quash is unavailing."[3]

Key Takeaways

The *Glassdoor* decision has significant implications for online, user-based platforms that provide their users with a veil of anonymity. Some fear that the decision may have a chilling effect on online speech, given that many users of online platforms are strangers to each other and, under this Ninth Circuit ruling, not entitled to the protections of associational privacy under the First Amendment.

Return to Table of Contents

[3] *In Re Grand Jury Subpoena*, No. 17-16221 (9th Cir. filed Nov. 8, 2017). A copy of the decision may be found here.

United Kingdom's National Audit Office Releases Report on Effects of WannaCry Cyberattack

Five months after the broad-based WannaCry ransomware attack, the U.K.'s National Audit Office released a postmortem report on the effects of WannaCry on England's National Health Service. The October 2017 report revealed that the debilitating effects of the attack could have been mitigated through the adoption of basic cybersecurity measures.

Five months after the broad-based WannaCry ransomware attack, the U.K.'s National Audit Office released a postmortem report on the effects of WannaCry on England's National Health Service. The October 2017 report revealed that the debilitating effects of the attack could have been mitigated through the adoption of basic cybersecurity measures.

On May 12, 2017, a global ransomware attack known as WannaCry simultaneously paralyzed more than 200,000 computers in more than 150 countries. Once a computer was infected, the attack's malware encrypted the data on the computer and demanded users pay $300 in order to regain accesss. Among those systems affected included computer systems operated by more than a third of the United Kingdom's National Health Service (NHS) trusts, the regional bodies that run the NHS. As a result of the attack, more than 6,900 NHS appointments were cancelled, though NHS has stated that it believes no patient data was compromised or stolen.

A U.K. National Audit Office (NAO) report was commissioned to investigate the effects of the attack, with the final report being released on October 27, 2017. NAO's key findings included:

- **NHS had been warned about cyber risks but had not taken action.** NHS trusts did not heed warnings from the U.K. Department of Health to update software and patch their systems. The trusts relied on outdated and sometimes unsupported software and failed to properly manage computer firewalls.
- **Department of Health leadership did not sufficiently emphasize cybersecurity management or allocate sufficient resources.** The Department of Health lacked both the ability to assess and the enforcement capacity to ensure compliance with its cybersecurity guidance. Moreover, responsibility for cybersecurity preparedness was deeply devolved throughout the organization. The NAO report also found evidence of insufficient funding for cybersecurity measures.

- **The Department of Health's critical incident response plan was not properly implemented.** Although the Department of Health had developed a cybersecurity incident response plan that included the roles and responsibilities of national and local organizations in responding to an attack, this plan had never been tested at a local level. As a result, there were no clear guidelines on who should lead the response and who should be contacted to report the cybersecurity incident. This, coupled with the shutdown of NHS computer systems, led to a breakdown in communications during the WannaCry attack.
- **NHS had a lack of understanding of the nature of cybersecurity risks.** In general, NHS trusts did not identify cybersecurity as a risk to patient outcomes and tended to overestimate their preparedness in the event of a cybersecurity event.

NAO concluded that the effects of the WannaCry ransomware attack on NHS were indicative of cybersecurity-related failures throughout the system. At a local level, trusts did not implement basic security measures that could have protected their computer systems from the attack. Additionally, at the management level, there was insufficient oversight and ability to monitor and enforce compliance.

NHS is now working on improving its cybersecurity protective measures through a series of steps:

- developing a more complete response plan;
- implementing a more robust system for reviewing and applying patches and antivirus updates;
- establishing a path for essential communications in emergency situations; and
- ensuring that all levels of the organization appreciate the scope of potential cybersecurity risks.

Key Takeaways

For all organizations, the WannaCry ransomware attack should serve as a reminder of the need to develop, monitor and enforce compliance with cybersecurity policies; ensure accountability for cybersecurity matters across all organizational levels, including management; and develop and test a critical incident response system — to include situations in which the attack itself makes normal means of communication and coordination difficult. These foundational steps are critical to ensure that an organization establishes basic cybersecurity best practices such as regularly installing software updates and properly maintaining system firewalls. These best practices may seem routine, but as the NAO report reminds readers, no organization should assume such steps are being taken, and they may prove vital to reducing an organization's cyber vulnerabilities.

Return to Table of Contents

White House Details US Government's Cost-Benefit Analysis for Releasing Zero-Day Vulnerabilities

The White House released a description of the process by which the U.S. government conducts a cost-benefit analysis in determining whether to release descriptions of previously unknown vulnerabilities in information systems and technologies used by commercial entities so that they may be patched, or withhold the information for use by law enforcement for national security purposes.

On November 15, 2017, the White House released the Vulnerabilities Equities Process (VEP) Charter, which describes the U.S. government's process for determining whether and how to release newly discovered vulnerabilities that are unknown publicly in information systems and technologies (*i.e.*, zero-day vulnerabilities).[4] The newly released document provides much greater transparency into a previously opaque process, lists the participating government agencies and describes the equities considered by the agencies. The release comes after the leak of reported National Security Agency hacking tools that used these types of vulnerabilities earlier this year, which resulted in the WannaCry ransomware attack.[5]

The VEP's stated focus is to prioritize the disclosure of zero-day vulnerabilities in order to protect critical infrastructure, information systems and the U.S. economy unless there is a "demonstrable, overriding interest in the use of the vulnerability for lawful intelligence, law enforcement, or national security purposes." The VEP accomplishes this cost-benefit analysis through consideration of four equities, as they apply to the present and near-term future:

[4] The VEP Charter is available here.

[5] Skadden's update on the SEC's cybersecurity risk alert on WannaCry is available here.

- defensive equities: the scope of the threat of exploitation, the potential impact of the vulnerability if exploited, and the availability and effectiveness of means of mitigating the vulnerability;
- intelligence, law enforcement and operational equities: the operational impact, value and effectiveness of the exploitation of the vulnerability as applied in intelligence activities, evidence collection and cyber operations;
- commercial equities: the risks posed to government relationships with industry if pre-existing government knowledge of the vulnerability is later revealed; and
- international partnership equities: the risks posed to U.S.-international relations if pre-existing government knowledge of the vulnerability is later revealed.

In balancing the above equities, the result of a VEP review is not limited to complete disclosure or retention. The process allows the government to take a range of options in tailoring the response to the identified equities, such as disseminating mitigation information without disclosing the vulnerability, limiting U.S. government use of the vulnerability, informing U.S. and allied government entities of the vulnerability at a classified level and/or indirectly informing an affected vendor of the vulnerability.

The National Security Council staff coordinates the VEP, but the Equities Review Board (ERB), which is responsible for deliberating on the above equities, includes a wide range of member agencies — from law enforcement, military and intelligence agencies to agencies with broad equities like the Departments of State and Commerce. Disputes between agencies over the preferred use of a vulnerability are resolved through the National Security Council and Homeland Security Council processes.

Supporting its stated focus on disclosure of vulnerabilities, if the ERB decides to restrict disclosure of a vulnerability, the VEP requires the vulnerability to be reassessed annually until it is either disseminated, publicly known or otherwise mitigated. While the VEP improves the transparency of the vulnerability review process and encourages disclosure, it still allows the government to exclude vulnerabilities from review that fall within certain specified categories, such as those used in sensitive operations. The details of these categories, including the number of categories and their breadth, are classified and have not been included in the release of the VEP.

Key Takeaways

The increased transparency and focus on disclosure of zero-day vulnerabilities should be considered a welcome development for information technology vendors and service providers. The updated process and focus on disclosure provide an opportunity for those vendors and service providers to engage with selected government partners to discuss potential vulnerabilities in their products and services, and develop relationships that may help them avoid the risk of future exploitation. Given the increased pressure on the government to maintain its leadership in cyber exploitation, establishing relationships with key participants in the VEP process may become a necessity for vendors and service providers hoping to ensure that the U.S. government recognizes the scope of potential defensive and commercial equities associated with a given set of products or services.

As with the previously mentioned NAO report, the VEP Charter also should serve as an important reminder to all organizations that routine and consistent patching of systems is a vital aspect of cybersecurity. The disclosure of security vulnerabilities through the VEP process or otherwise is only the first step to improved cybersecurity. As noted above, many organizations suffered far greater effects from the WannaCry malware because they had not fully adopted available security patches.

Return to Table of Contents

Surveillance Court Rules ACLU and Yale Clinic Have Standing to Pursue Release of Section 215 Rulings

In its first public *en banc* ruling, a United States surveillance court ruled that parties could have access to surveillance court judicial opinions related to programs permitting the bulk collection of communications information.

On November 9, 2017, the Foreign Intelligence Surveillance Court (FISC) ruled the American Civil Liberties Union (ACLU) and Yale Law School's Media Freedom and Information Access Clinic (MFIA Clinic) have standing to proceed with their suit to compel the release of FISC opinions evaluating the meaning, scope and constitutionality of Section 215 of the USA Patriot Act, 50 U.S.C. § 1861. FISC's prior approval of the surveillance requests under Section 215 led to the bulk collection of American citizens' telephonic metadata from telecommunications companies for use in counterterrorism efforts.

The ACLU and MFIA Clinic filed a motion to release the legal reasoning for the approval of the Section 215 requests in 2013 shortly after two newspapers published classified information about U.S. government surveillance programs. Within a day of publication, the director of national intelligence declassified

other details of the bulk data collection program and acknowledged the FISC had authorized the actions under Section 215. After the declassification reviews, the parties sought access to the redacted material. U.S. District Judge Rosemary M. Collyer ruled in January that citizens do not have a First Amendment right to read the FISC's full court decisions pertaining to the National Security Agency's bulk data collection program.

In vacating Judge Collyer's decision and remanding the case to her chambers to rule on the merits, the majority found the four judicial opinions sought by the parties should be considered "legal proceedings" to which the parties could claim access under the First Amendment. With a 6-5 majority, this case marked the first *en banc* ruling where all 11 FISC member judges participated in the decision. The majority opinion, written by U.S. District Judge James E. Boasberg, cited *Richmond Newspapers, Inc. v. Virginia*, 448 U.S. 555 (1980), which recognizes the right of access to court proceedings and documents. Judge Boasberg noted the parties' claim here "survives because the injury is a lack of access to the proceedings of a court" rather than an executive branch function in foreign affairs. Writing for the dissent, Judge Collyer defined the parties' request not as "access to judicial proceedings" but rather a "'right' of access to the information classified by the Executive Branch," upsetting the separation of power between the judiciary and executive branches.

Key Takeaways

Private entities regularly receive requests from federal agencies for access to stored information or other tangible items under Section 215, but in most cases they receive only very limited guidance regarding the scope of their required disclosures. By establishing the potential viability of a claim to access FISC proceedings, this case eventually could lead to the release of additional judicial guidance on the scope of Section 215 and accordingly provide additional counsel to companies with related compliance concerns. Although this decision does not provide for the public release of FISC opinions — rather, it merely provides that parties have standing to pursue such a claim — it at least offers a potential judicial path given that the court allowed the claim to go forward.

Return to Table of Contents

District Court Holds That Insurer's Written Privacy Pledge to Insured is Unenforceable in Data Breach Row

In a victory for insurers, a federal court recently determined that a privacy pledge included with an insurance policy is not considered part of the policy and therefore was not enforceable against the insurer in a data breach dispute with its insured stemming from the insurer's alleged failure to adequately safeguard the insured's personal information.

On November 8, 2017, the U.S. District Court for the Northern District of Illinois granted summary judgment in favor of Combined Insurance Company of America (Combined), the health insurer of department store chain Dillard's, in a data breach dispute with a Dillard's employee. The court concluded that a privacy pledge included with the employee's insurance policy did not form part of the contract and therefore was not enforceable against Combined.[6]

The Data Breach Lawsuit

In May 2014, plaintiff Ann Dolmage commenced a putative class action against Combined on behalf of herself and similarly situated individuals in the Northern District of Illinois after it was discovered that Enrolltek, a third party vendor hired by Combined, failed to adequately secure its website and, as a result, the personal identifiable information (PII) of Dolmage and thousands of other insured Dillard's employees was publicly accessible on the internet for over a year. The lawsuit alleged that Combined breached the privacy pledge included with Dolmage's policy by failing to ensure that Enrolltek securely maintained her PII. The privacy pledge, which was included in all Dillard's employee enrollment packages, stated that Combined would protect her PII, including to the extent it is shared with third parties.

In August 2017, Combined moved for summary judgment on Dolmage's breach of contract claim on the basis that, in Combined's view, the privacy pledge was not part of Dolmage's

[6] *Dolmage v. Combined Ins. Co. of Am.*, No. 14 C 3809, 2017 WL 5178792 (N.D. Ill. Nov. 8, 2017). A copy of the decision can be found here.

policy. Dolmage opposed the motion, arguing — in reliance on a definitional provision in the policy stating that "policy means this policy with any attached application(s), and any riders and endorsements" — that the Privacy Pledge is part of her policy because it is a rider or endorsement that was incorporated by reference into the policy.

The Court's Ruling on the Enforceability of the Privacy Pledge

The court sided with Combined, holding that "the Privacy Pledge is not a rider or endorsement that was incorporated by reference into the policy, and thus the Privacy Pledge did not create a legally enforceable promise." The court relied on an expert opinion proffered by Combined, which identified various "hallmarks" of an insurance policy rider or endorsement: being clearly marked as a rider or endorsement, being signed by an official of the insurance company and expressly referencing the policy in question. "The Privacy Pledge does not bear any of these hallmarks," the court observed. The court also pointed to the fact that the enrollment materials included an "accelerated payment rider" to the policy, which, in sharp contrast to the privacy pledge, was clearly labeled as a policy rider, signed by Combined executives and expressly stated that the rider was part of the policy.

The court rejected Dolmage's argument that the privacy pledge formed part of the policy simply because it was included in the same package as the policy. Accepting Dolmage's position, the court reasoned, would mean that all enrollment documents (including blank forms and informational brochures) provided with the policy — documents that do not bear any indicia of true riders or endorsements — would automatically form part of the policy, which clearly was not intended. Accordingly, the court granted summary judgment in favor of Combined.

Key Takeaways

It is unclear whether other courts, if and when they are faced with privacy pledges included in or with insurance policies, will reach conclusions similar to those reached in *Dolmage v. Combined Insurance*. As the court's decision illustrates, the issue likely will turn on the language of the policy and the privacy pledge at issue, as well as the manner in which the pledge is presented to the insured. A finding of enforceability by other courts could have meaningful implications for future data breach disputes, as privacy pledges are becoming more common in enrollment packages in which PII is collected.

Return to Table of Contents

SWIFT Report Highlights Changing Cyber Threat Landscape for Financial Institutions

In October 2017, the SWIFT Institute published a working paper, "Forces Shaping the Cyber Threat Landscape for Financial Institutions"[7] (the paper), that examines the evolving tactics and tools used in cybercrime against financial institutions and outlines several recommendations for financial institutions to combat cyber threats more effectively.

New Tools and Tactics for Cybercrime

The paper notes that advances in technology, new developments in fraud detection and prevention, and changing incentives for attackers have resulted in attackers using new tools and tactics in cybercrimes against financial institutions.

With respect to consumer fraud, the paper explains that the advent of multi-factor authentication and chip cards has forced fraudsters to seek different approaches, including, for example, large-scale attacks on point-of-sale systems. Business email compromise tactics (*e.g.*, where fraudsters send fake emails to employees pretending to be their manager and directing them to make cash transfers from the companies' accounts) also have increased dramatically. The increase in mobile banking has provided another avenue for cybercrime attacks, and studies have shown that mobile malware attacks and mobile banking Trojans have increased exponentially over the last few years. Furthermore, as internet and mobile banking expand to emerging markets, one byproduct is that the geography of cybercrime also is expanding, as billions of new internet users (often with little cybersecurity awareness or access to security products) have become easy targets for cyberattacks.

In addition to consumer fraud, cyber criminals are also increasing efforts to carry out targeted attacks against bank networks. The paper explains that these attackers have become much more sophisticated in recent years, with nation-state hacking groups increasingly becoming involved in cybercrimes against financial institutions. Furthermore, capabilities that once were only available to nation-states have become increasingly available to criminal organizations, with hacking tools stolen from intelligence agencies and other sources becoming widely available via open-source malware libraries. As fraudsters have become more sophisticated, law enforcement is struggling to keep up with changes in technology and the broad adoption of encryption.

[7] A copy of the paper can be found here.

With respect to the specific tools and tactics used to target bank networks, the paper notes that manipulating insiders remains the number one way that banks often become compromised, explaining that as phishing attacks become less effective due to successful "don't click the link" campaigns, attackers have turned to social engineering to convince unwitting victims, such as bank employees, to provide hackers with access to their computers. Watering hole attacks (*i.e.*, attacks where the attacker compromises a website that the attacker knows their target will visit and then uses that site to infect the target's system with malware) also have increased in frequency and sophistication level, in addition to dedicated denial-of-service attacks from internet-of-things botnets and ransomware activity. Additionally, the paper explains that the same machine learning approach used to detect patterns for cybersecurity defense can be used by attackers to select targets, and it is only a matter of time before machine learning is incorporated into the cyberattacks themselves. Another trend that the paper highlights is the selective targeting of less sophisticated financial institutions by criminals to gain access to more well-defended networks, noting that financial institutions in Asia are particularly vulnerable to attack and are less likely to have invested significantly in cyber defenses.

Key Takeaways

The paper makes the important point that each financial institution must consider cybersecurity within the larger context of the global network of financial institutions and makes the following suggestions for financial institutions to combat the cybercrime tactics summarized above:

- strengthen global financial institution networks by ensuring that small and medium financial institutions in emerging markets build cyber awareness and security capacities to prevent exploitation of these banks by cyber attackers; and
- support efforts to secure the broader ecosystem. In order to defend against internet and mobile banking threats, banks should strengthen authentication and monitoring for devices that connect to their systems, help build law enforcement capacity to combat cybercrime and improve education efforts regarding cybercrime.

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

Michael Y. Scudder
Partner / Chicago
312.407.0877
michael.scudder@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

Joshua F. Gruenspecht
Associate / Washington, D.C.
202.371.7316
joshua.gruenspecht@skadden.com

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