Skadden

Privacy & Cybersecurity Update

US Chamber of Commerce and Business Groups Urge Congress to Pass Privacy Legislation

The U.S. Chamber of Commerce and various business groups have sent a letter to Congress advocating for comprehensive federal privacy legislation, citing the difficulty of complying with multiple state laws.

On January 13, 2022, the U.S. Chamber of Commerce and a wide array of trade groups delivered a letter to Congress imploring the legislative body to act on a federal privacy standard.[1]

The Chamber was joined in signing the letter by nearly 100 national and regional industry organizations and local chambers of commerce, including the Consumer Data Industry Association, the Foodservice Equipment Distributors Association, TechNet and the Software & Information Industry Association. The letters referenced the "growing patchwork of state laws" — specifically, the California Consumer Privacy Act, the California Privacy Rights Act and laws passed in Virginia and Colorado — that each entail different approaches to enforcement, duties and scope. The letter also noted the Federal Trade Commission's contemplated privacy rulemaking as adding another layer of complexity. These differing approaches, the groups argued, threaten innovation and create consumer and business confusion, while also making compliance "incredibly difficult" for small businesses.

To alleviate these burdens, the letter urged Congress to pass a single national standard, which would provide meaningful and robust protections for consumers and would limit enforcement to federal agencies and state attorneys general.

Key Takeaways

Industry calls for comprehensive national privacy legislation are not new, but the letter is notable for the wide range of industry groups signing on, for its discussion of the difficulties posed by multiple different state privacy laws and for underscoring the growing desire among private business and industry groups for streamlined federal privacy legislation. While momentum grows among states to continue passing their own unique privacy laws, national businesses are likely to keep pushing for preemptive federal legislation that simplifies and reduces the costs of compliance.

Return to Table of Contents

[1] The letter is available here.

District Court Rules General Liability Insurer Has No Duty to Defend Insured in Illinois Biometric Information Privacy Act Suit

A federal judge ruled that general liability insurer American Family Mutual Insurance Company, S.I. (American Family) had no duty to defend its insured Caremel Inc. (Caremel), an operator of multiple McDonald's locations in Illinois, in a lawsuit alleging violation of the Illinois Biometric Information Privacy Act (BIPA), a privacy law that imposes restrictions on how private entities collect, store and dispose of identifying biometric information.

On January 7, 2022, U.S. District Judge Harry D. Leinenweber of the Northern District of Illinois granted American Family's motion for summary judgment in a coverage action against its insured, Caremel, holding that the insurer had no duty to defend the company in an underlying putative class action alleging BIPA violations on the basis that an exclusion in Caremel's insurance policy barred coverage.[2]

The Underlying BIPA Suit

In 2019, Joseph Ross, an employee at one of Caremel's McDonald's locations, filed an action in the Circuit Court of Kankakee County, Illinois against Caremel alleging that it violated BIPA. The complaint alleged that Caremel required Mr. Ross and other McDonald's employees to scan their fingerprints in order to clock in and out of work. This identifying information allegedly was disclosed to Caremel's third-party timekeeping vendor without the employees' consent. Mr. Ross alleged that Caremel's disclosure of this identifying information to its timekeeping vendor violated BIPA.

Caremel's Insurance Claim

At the time the suit was filed, American Family insured Caremel under a businessowners insurance policy that, as relevant here, provided coverage for "sums the insured becomes legally obligated to pay as damages because of ... 'personal and advertising injury'" and included a duty to defend potentially covered suits. Caremel sought coverage under the policy for the underlying BIPA suit. American Family denied coverage, invoking three policy exclusions: (1) the Access and Disclosure Exclusion, which bars coverage for "access or disclosure of confidential or personal information and data related to liability"; (2) the Violation of Statute Exclusion, which bars coverage for claims resulting from the distribution of materials in violation of statute; and (3) the Employment Related Practices Exclusion (ERP Exclusion), which bars coverage for personal and advertising injury arising out of employment related practices, policies, acts or omissions directed at the individual.

American Family's Declaratory Judgment Action

In January 2020, American Family filed suit against Caremel in the Northern District of Illinois seeking a declaratory judgment that the insurer had no duty to defend Caremel in the underlying BIPA suit. In July 2021, American Family moved for summary judgment.

District Court Grants Summary Judgment in Favor of American Family

In January 2022, the district court granted American Family's motion for summary judgment, holding that the ERP Exclusion applied to bar coverage for the underlying BIPA suit. In so holding, the court accepted American Family's argument that the requirement that an employee give his fingerprints is an employment-related practice. The court rejected Caremel's argument that the ERP Exclusion was inapplicable because it applied to practices directed at individual employees and the fingerprint requirement was directed to all employees. "[T]he requirement that an employee submit his fingerprints is a requirement that applies to employees individually" and each employee "suffer[s] risk of individual injuries," the court found. The court also rejected Caremel's *ejusdem generis* argument that a BIPA violation is unlike the exemplar employment-related practices listed in the ERP Exclusion, reasoning that "[e]ach of 'coercion, demotion, evaluation, reassignment, discipline, defamation, harassment, humiliation or discrimination directed at a person' reflect a practice that can cause individual harm to an employee ... the same is true for a BIPA violation." The court also considered and rejected American Family's arguments with respect to the Access and Disclosure Exclusion and the Violation of Statute Exclusion.

Key Takeaways

As states continue to enact legislation aimed at protecting individuals against privacy violations, policyholders and insurers alike would be well-advised to revisit the terms of their insurance contracts to ensure that the parties have a clear and mutual understanding of the scope of coverage provided for such actual and alleged privacy violations.

Return to Table of Contents

[2]The decision is *Am. Family Mut. Ins. Co. v. Caremel, Inc.*, 20 C 637 (N.D. Ill. Jan. 7, 2022).

New York Attorney General Warns Companies of Unavoidable and Ubiquitous 'Credential Stuffing' Attacks

New York Attorney General Letitia James reported that "credential stuffing" attacks compromising more than 1.1 million customer accounts had occurred across a variety of companies and provided guidance on how to defend against these attacks.

On January 5, 2022, the Office of the New York Attorney General announced the results of an investigation into so-called "credential stuffing" attacks. The investigation found that more than 1.1 million customer accounts had been compromised by these types of attacks across at least 17 well-known — but unidentified — companies. According to the investigation, credential stuffing attacks are unavoidable for most businesses, and every business that maintains online customer accounts must have safeguards in place to detect and prevent these attacks. As such, the office released a guide detailing safeguards that businesses should implement to protect against these attacks.

Credential Stuffing

Credential stuffing is a relatively simply cyberattack, in which hackers use credentials stolen from one online service provider to access users' other online accounts. Because people tend to reuse passwords across multiple accounts, once a password is compromised on one service, hackers can leverage this information to attempt to login to other websites. According to the attorney general's office, lists of stolen usernames and passwords are readily accessible on the dark web and other hacking forums. Using these lists of credentials, hackers deploy easily accessible software to transmit hundreds of login requests simultaneously. While the vast majority of these attempts do not succeed, through the sheer volume of attacks (often in the millions) these efforts can easily yield thousands of successful hits.

Once a hacker gains access to an account, it can monetize the compromised account in multiple ways. For example, they may use saved payment information to make fraudulent purchases, steal other personal data for use in further phishing attacks, or sell the login credentials to other bad actors on the dark web.

Results of the Attorney General's Investigation

The attorney general's office conducted an investigation to identify businesses and consumers that had been compromised by credential stuffing attacks. By monitoring online communities dedicated to credential stuffing over a period of several months, the investigation uncovered thousands of posts containing affirmatively tested customer login credentials. These verified credentials were available for any other community member to use, either to break into the same account or to use for future attacks on other websites and applications. In total, the attorney general's office discovered credentials for more than 1.1 million customer accounts, all of which were apparently obtained via credential stuffing attacks. These included customer accounts at 17 online retailers, restaurant chains and food delivery services. The affected companies worked with the attorney general's office to investigate how hackers had overcome existing safeguards and to implement enhanced data security programs.

Notably, the attorney general's office found that credential stuffing attackers were able to circumvent common security measures. For example, some attackers evaded web-based application firewall measures by disguising the source of the login attempt. By using multiple proxy IP addresses, credential stuffing attacks evaded rate-limiting measures that block traffic from users attempting to login to multiple customer accounts in quick succession. Other attackers used fraudulently obtained account information to outsmart authentication mechanisms. At certain companies, orders placed to a new address using stored credit card information required customer reauthentication, while orders placed to a new address using store credit did not. Malicious actors also circumvented the reauthentication security measures by placing orders to customers' existing addresses, then cancelling these orders and using the resulting store credit to place an order to a new address.

Combating Credential Stuffing Attacks Requires Proactive Cybersecurity Measures

In order to better secure customer accounts against credential stuffing attacks, the attorney general's office recommended safeguards that it viewed as highly effective, including: (1) monitoring customer activity through bot detection services, (2) utilizing multifactor and password-less authentication, and (3) requiring reauthentication at the time of purchase. The attorney general recommended that companies maintaining online customer accounts implement these and other measures to defend against this attack vector, detect credential stuffing breaches, prevent fraudulent use of comprised customer information and allow for timely responses to attacks. These methods are outlined below.

- **Multifactor and Password-Less Authentication.** Multifactor authentication requires at least two different types of authentication to login. The attorney general's office advised that credential stuffing attackers that have access to a stolen password likely will not be able to circumvent these additional authentication factors. Similarly, password-less authentication does not require a customer password. Customers are instead authenticated via alternative authentication mechanisms, such as one-time passwords and authenticator apps.

- **Bot Detection Services.** Bot detection systems identify and block internet traffic generated by automated software, or "bots." Since credential stuffing utilizes automated software to launch thousands of login attempts, the attorney general's office indicated that bot detection software can be highly effective at mitigating and detecting these attacks. The report stated that one company's bot detection vendor had blocked over 271 million login attempts over a 17-month period, while another company reported over 40 million login attempts blocked over a two-month period. Third-party bot detection service providers may be preferable to in-house software, as such services have access to a larger amount of data and can identify suspicious patterns that may not be apparent to any single website operator.
- **Reauthentication at Time of Purchase.** Once a credential stuffing attacker has accessed a customer's account, reauthenticating at the time of a purchase prevents such attackers from making fraudulent purchases. Companies may require that the customer reauthenticate their stored payment information, for example by reentering the CVV code on their credit card, or may reauthenticate the customer, such as through one-time passwords or links. The report recommended that businesses should implement reauthentication measures for each payment method that they accept, including gift cards, loyalty points and store credit.

In addition, the report recommended that businesses implement a response plan to investigate, remediate and notify customers in the event of a credential stuffing attack.

Key Takeaways

As the attorney general's office report found, credential stuffing is an increasingly prevalent form of cyberattack that can be difficult to defend against using common cybersecurity measures. Companies that maintain customers' account information should review their cybersecurity programs to see whether they include effective measures to detect and prevent these attacks. In particular, companies should carefully consider the report's specific cybersecurity recommendations, as plaintiffs' lawyers could use these recommendations in negligence or other claims as an indication of what companies should be doing to prevent these types of attacks.

Return to Table of Contents

FTC Warns Companies to Remediate Log4j Security Vulnerability or Face Action

The Federal Trade Commission (FTC) has warned companies that failing to address a widely known vulnerability could lead to FTC action against them.

On January 4, 2022, the FTC issued a statement advising companies to take steps to mitigate the threat posed by the high-profile Log4j vulnerability or face penalty from the commission.[3] The vulnerability has been found in a popular piece of software that is used across many industries and applications, and poses a "severe risk" to consumers as the FTC says it is being "widely exploited" by a growing set of attackers.

Background

Log4j is a popular open source Java logging library that is incorporated in a wide array of mobile applications, enterprise software and consumer products, such as smart TVs and internet-connected security cameras. The first reports of a critical security vulnerability in the software came to light in December 2021. The vulnerability has potentially exposed millions of devices worldwide to hacking attempts and other security breaches.

FTC's Role and Warning

The FTC Act bars "unfair or deceptive acts or practices in or affecting commerce" and grants enforcement power to the commission. The FTC has historically taken the view that poor cybersecurity practices can lead to breaches of personal information, financial loss and other harms to consumers, and can therefore rise to the level of constituting unfair business practices prohibited by the FTC Act.

On January 4, 2022, the FTC issued a statement warning companies and their vendors that rely on Log4j to remedy the exposure or face enforcement action. The commission reminded companies of the case of Equifax, which in 2019 agreed to pay $700 million to settle actions by the FTC, the Consumer Financial Protection Bureau and all 50 states after failing to patch a 2017 vulnerability that exposed the personal information of 147 million consumers. In its announcement, the FTC issued the following stark warning:

> **"The FTC intends to use its full legal authority to pursue companies that fail to take reasonable steps to protect consumer data from exposure as a result of Log4j, or similar known vulnerabilities in the future."**

[3] The FTC's announcement is available here.

FTC Recommendations

The FTC recommends four main actions to remediate the Log4j vulnerability:

- update the Log4j software package to the most current version;
- consult the Cybersecurity and Infrastructure Security Agency's guidance to mitigate the Log4j vulnerability;
- ensure remedial steps are taken to ensure that the company's practices do not violate the law, noting that failure to identify and patch Log4j may violate the FTC Act; and
- distribute information about the vulnerability and remedies to relevant third-party subsidiaries that sell products or services to consumers that also may be vulnerable.

Key Takeaways

Through its announcement, the FTC is making clear that it intends to pursue companies that have failed to act to remediate the Log4j issue. This announcement — though somewhat unusual in it specificity — is consistent with the commission's general approach to protecting consumers against unfair cybersecurity practices: failing to patch a known critical vulnerability that exposes consumers to harm is, in the FTC's view, a violation of the FTC Act. To protect consumers and lower the risk of an FTC action, companies should continue to monitor for widespread vulnerabilities, take swift corrective action when necessary, and make sure its vendors also are appropriately mitigating and remediating risks.

Return to Table of Contents

Health Trade Association Releases Medical Device and Service Cybersecurity Guidance

The Healthcare Supply Chain Association (HSCA), a trade association that represents the interests of the health care industry, outlined certain key cybersecurity recommendations for medical device manufacturers, health care delivery organizations and service providers.

On December 21, 2021, the HSCA published its recommended cybersecurity guidelines for medical device manufacturers.[4] Citing the recent widespread adoption of telemedicine and the rapid shift to virtual operations during the COVID-19 pandemic, the HSCA highlighted the valued role of information technology in patient care, as well as the unique vulnerabilities that medical devices and services present with respect to patient health, safety and privacy. The published guidelines emphasize the shared responsibility of device manufacturers, suppliers and health care delivery organizations to maintain device and information security against cybersecurity threats to ensure the privacy of patient data.

Healthcare Supply Chain Association

The HSCA is a trade association that represents health care group purchasing organizations across the United States and advocates for improved efficiency in the purchase and sale of health care goods and services. Members of the HSCA include hospitals, long-term care facilities, surgery centers, clinics and other "healthcare delivery organizations" (HDOs). The HSCA's vantage point over the entire health care supply chain enables the group to assess the interconnectivity of cybersecurity risks and to advocate for a coordinated approach to managing such risks across the health care industry.

The Recommendations

The HSCA's new cyber guidelines focus on four main classes of consideration:

- cybersecurity training and software;
- equipment acquisition standards and risk coverage;
- data encryption; and
- information sharing and standards organizations.

The HSCA provided tips for industry participants to identify red flags before doing business with a new organization. At minimum, the HSCA recommends that HDOs and suppliers:

- participate in at least one information sharing and analysis organization (*e.g.*, the Health Information Sharing and Analysis Center);
- utilize an information technology security risk assessment methodology; and
- align their practices with widely accepted standards (*e.g.*, from the National Institute of Standards and Technology).

The HSCA also recommended additional commonplace cybersecurity measures and practices for organizations to implement, such as designating an information security officer, ensuring that employees receive role-appropriate periodic training and assessments on cybersecurity, implementing anti-virus software and firewalls, and promptly patching and updating all software, firmware and third-party applications.

The HSCA also advised that device manufacturers state the expected useful life of a device (or service) within the appli-

[4]The HSCA's recommendations are available here.

cable purchase agreement, and provide security updates to the software and all supporting software components for that stated useful life at no further cost to the HDO. Further recommended contract terms are set forth in a separate guide promulgated by the HSCA.[5] In addition, certain key measures recommended by the HSCA are specific to HDOs or medical device suppliers, as described below.

For HDOs

The HSCA advised HDOs against working with any manufacturer that does not actively participate in an information sharing and analysis organization, given the importance of information sharing in improving cybersecurity for all community participants. HDOs should also avoid acquiring devices from a supplier which is unwilling to provide a recent Manufacturer Disclosure Statement for Medical Device Security or which devices or services are not in compliance with current U.S. Food and Drug Administration (FDA) cybersecurity guidance.

The HSCA also advised that health care organizations should ensure that their insurance policies cover cybersecurity risks with appropriate minimum coverage (and should generally not acquire devices or services from suppliers who refuse to provide evidence of appropriate coverage), while also ensuring purchase agreements for medical devices and services include appropriate liability and warranty provisions.

For Medical Device Manufacturers and Service Suppliers

The HSCA encouraged suppliers to provide a software bill of materials for any medical device that can be connected to a network, maintain a cyber insurance policy with appropriate minimum coverage and ensure compliance with current FDA guidance. It encouraged adherence to all federal regulations, including quality system regulations, and stated that such compliance should be viewed as a precondition to marketing any medical device. Suppliers should make every effort to assist HDOs in resolving cyber vulnerabilities in a timely manner, including providing reliable information and guidance on how to address vulnerabilities.

With respect to the ongoing risks posed by legacy devices that may not be compliant with current cybersecurity guidelines, the HSCA recommended that manufacturers acknowledge their responsibility for the security of such devices and work to upgrade them to current security standards (or otherwise provide device upgrade paths to HDOs at the lowest possible cost), in light of the difficulty for HDOs to discontinue or replace such devices.

[5]The HSCA's "Recommendations for Medical Device Cybersecurity Terms and Conditions" are available here.

Key Takeaways

The existence of industry self-guidance such as that of the HSCA can be both a blessing and curse for industry participants. In light of the ongoing lack of comprehensive cybersecurity laws or standards, this type of guidance can be a valuable source of information on industry best practices, and can be useful to device purchasers in setting expectations with manufacturers. On the other hand, even if organizations have no formal legal obligation to comply with these recommendations, plaintiffs' lawyers could accuse an organization of negligence or other wrongdoing if it experiences a cybersecurity incident that could have been prevented had it followed the guidance. Further, industry self-regulation can serve additional industry interests, as adoption of an effective self-determined standard may reduce the pressure on legislators to pass federal (or state) laws in the same area. For all of these reasons, industry participants should carefully consider applying these standards to their own practices.

Return to Table of Contents

UK Government Publishes National Cyber Strategy

The U.K. government has released a national strategy for cyberspace, outlining five major policy goals to solidify and enhance its standing among the world's privacy powers.

On December 15, 2021, the U.K. government published its National Cyber Strategy for 2022 (the strategy), which details the government's plan to solidify the U.K.'s position as a global cyber power.[6] The strategy replaces the government's National Cyber Security Strategy 2016-2021 and is based on five key pillars, which set out goals that the government intends to achieve by 2025. Together, the five pillars are intended to protect and promote U.K. interests in cyberspace and protect the U.K. from cyber threats.

The Five Pillars

Five pillars will guide and organize the specific actions that the government will take and the outcomes it intends to achieve by 2025. We outline these pillars, and certain of the specific actions the government intends to take under each, below:

1. **Strengthening the U.K. cyber ecosystem, investing in people and skills, and deepening the partnership between government, academia and industry.** To stimu-

[6]The Strategy can be found in full on the Government's website, available here.

late a more inclusive and strategic national cyber dialogue with industry, academia and citizens, the government intends to establish a new National Cyber Advisory Board, consisting of senior leaders from the public, private and third sectors, and will continue to work on improving integration between the U.K.'s 12 regional cyber clusters. To strengthen the U.K.'s cyber ecosystem, the government intends to introduce a number of higher education training courses and skills bootcamps in an effort to increase the number of young people entering into the cybersecurity profession. This will be furthered by the establishment of professional standards by the U.K. Cyber Security Council, underpinned by Royal Charter.

2. **Building a resilient and prosperous digital U.K., reducing cyber risks so businesses can maximize the economic benefits of digital technology, and making sure citizens are more secure online and confident that their data is protected.** The government intends to develop an up-to-date strategic understanding of the nation's cyber risk to ensure that it can identify systemic risk, communicate priorities, and drive strategy and delivery. In order to lead by example in its understanding of cyber risk, the government also plans to adopt the National Cyber Security Centre's Cyber Assessment Framework as an assurance framework to be adopted by all government departments, and the government's critical systems and common suppliers will be mapped. A new government Cyber Coordination Centre and cross-government Vulnerability Reporting Service also will be established to enable the government to "defend as one" when managing incidents, vulnerabilities and threats.
3. **Taking the lead in technologies that are vital to cyber power, building the U.K.'s industrial capability and developing frameworks to secure future technologies.** The government intends to prioritize, and take a leading role in the further development of, a range of technologies and applications that it deems are vital to cyber power. The strategy cites the following examples: 5G and 6G technology and other emerging forms of data transmission; artificial intelligence; blockchain technology and its applications, such as cryptocurrencies and decentralized finance; semiconductors and microprocessor chips; cryptographic authentication; the internet of things; and quantum technologies, including quantum computing, quantum sensing and post-quantum cryptography.
4. **Advancing U.K. global leadership and influence for a more secure, prosperous and open international order, working with government and industry partners, and sharing the expertise that underpins U.K. cyber power.** The government intends to take a more activist international leadership role to promote the U.K.'s interests and values in cyberspace. This will involve continuing to work with effective multilateral organizations and partnerships, including the United Nations, Five Eyes, NATO, the G7, the EU, the U.K. Commonwealth, the OECD, the Global Forum on Cyber Expertise, the ASEAN Forum, the African Union and the World Bank. To improve the protection of U.K. interests and citizens overseas, the government intends to develop and deliver an international cyber hygiene campaign for U.K. overseas missions, which will be delivered through the U.K.'s diplomats and country-based staff and aim to raise the cost of malicious activity, such as hacking, data and intellectual property theft and ransomware.
5. **Detecting, disrupting and deterring adversaries to enhance U.K. security in and through cyberspace, making more integrated, creative and routine use of the U.K.'s full spectrum of levers.** The government plans to develop a joint data access and exploitation strategy across the U.K.'s intelligence and law enforcement organizations to improve how threat detection is coordinated across government departments. To render a higher risk for penalty to state, criminal and other malicious cyber actors to target the U.K., the government plans to implement sustained and tailored deterrence campaigns. There also are plans to bolster the tools and powers available to law enforcement and intelligence agencies, such as by updating existing legislation and introducing new offenses to account for how state threats have evolved.

Key Takeaways

Through implementation of the strategy and, in particular, by taking the specific actions outlined under each of the five pillars, the government intends to strengthen the U.K.'s position as a global cyber power by 2025. The strategy is intended to serve as a platform for further engagement with the public, private and third sectors across the U.K., with direct feedback encouraged via email to ukcyberstrategy@cabinetoffice.gov.uk. The government intends to report back annually on the progress it is making to implement the specific actions detailed in the strategy.

Return to Table of Contents

Contacts

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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
One Manhattan West
New York, NY 10001
212.735.3000