Skadden

Privacy & Cybersecurity Update

FTC Updates Gramm-Leach-Bliley Act's Safeguards Rule

The Federal Trade Commission (FTC) has updated the GLBA Safeguards Rule to require nonbanking financial institutions to take a range of specific security measures, including encrypting customer information.

On October 27, 2021, the FTC revised its data security Safeguards Rule under the Gramm-Leach-Bliley Act (GLBA) to include a variety of specific technological and organizational security measures for nonbanking financial institutions, such as requiring them to encrypt customers' personal data and designate a cybersecurity lead within their organization.[1] These revisions — the first changes to the Safeguards Rule since it was adopted in 2003 — were first proposed in 2019, and were approved in a 3-2 vote over the vocal objection of two commissioners.

Background

The GLBA required that the FTC develop certain rules for the processing and protection of personal information by financial institutions within its jurisdiction, including for setting certain security standards. Pursuant to this mandate, in 2003 the FTC instituted its Safeguards Rule, which as a general matter required financial institutions under the FTC's jurisdiction to develop a written information security plan tailored to the institution's size, operations and complexity, as well as to the sensitivity of the customers' information. The rule generally did not dictate specific security measures for these institutions to take and instead required them to evaluate the risks they faced and design their security plan accordingly.

The rule applies to nonbanking financial institutions, such as mortgage lenders, pay-day lenders, finance companies, mortgage brokers, account servicers, check cashers, wire transferors, certain travel agencies, collection agencies, credit counselors and other financial advisors, and tax preparation firms.

Changes to the Safeguards Rule

The changes to the Safeguards Rule generally expand on the requirements of the existing rule, in some cases by requiring financial institutions to take specific technical

[1] The full Final Rule from the FTC is available here.

and organizational measures. The new requirements include obligations to:

- appoint a "Qualified Individual" to oversee, implement and enforce the information security program;
- use encryption to secure consumer information;
- use multifactor authentication for accessing information;
- implement access controls and authentication mechanisms to limit access to consumer data;
- adopt secure development principles for in-house software development;
- develop procedures for the secure disposal of customer information within two years after it was last used; and
- conduct annual penetration tests.

The revised Safeguards Rule exempts certain smaller organizations — those that collect information on fewer than 5,000 consumers — from certain internal process requirements.

In general, though the changes impose new requirements for financial institutions' information security plans, they do not dictate the specific means by which they should be implemented, leaving some room for flexibility. Nevertheless, some have criticized the changes as a departure from the FTC's prior approach of allowing financial institutions considerable discretion to adopt security procedures that best fit the risks they face.

Key Takeaways

Organizations subject to the FTC's Safeguards Rule should carefully review the expanded requirements. While many of the changes reflect what have developed into industry standard practices over the nearly two decades since the rule was initially adopted, organizations should ensure that they meet each of the specific new requirements.

Return to Table of Contents

CFPB Issues Orders To Gather Information From Tech Companies Regarding Consumer Payment Products

The Consumer Financial Protection Bureau (CFPB) is requiring six of the largest technology firms to provide information on payment products, plans and practices.

On October 21, 2021, the CFPB issued market-monitoring orders to six major technology companies that operate payment platforms, calling for information regarding payment products, plans and practices, including with respect to their data collection practices. The orders are intended to inform regulators and policymakers about payments systems, and may also be used by the CFPB in future rulemaking in the payments industry.

Background

The Consumer Financial Protection Act authorizes the CFPB to take steps to monitor markets for consumer financial products and services.[2] While the CFPB's use of its market-monitoring authority is less common than its use of other tools, such as civil investigative demands and the supervisory process with respect to some institutions, the CFPB has used market-monitoring activities in the past to conduct research into areas such as remittances, student loan servicing and arbitration clause practices. The CFPB's typical previous practice has been to not publicly disclose the recipients of market-monitoring orders. In this case, however, the CFPB publicly released the identities of the firms that received the market-monitoring orders and a sample of the order sent to those firms.

In a press release on October 21, 2021, CFPB Director Rohit Chopra, who had been sworn in only a few days earlier, stated that while "[f]aster, friction-less, and cheaper payment systems offer significant potential benefits to consumers," payments businesses "can gain tremendous scale and market power, potentially posing new risks and undermining fair competition."[3] In addition, Mr. Chopra suggested that a focus of the market monitoring will address how consumer payments information is monetized in the market, stating "knowing what we spend our money on is a valuable source of data on consumer behavior. This data can be monetized by companies that seek to profit from behavioral targeting, particularly around advertising and e-commerce." In addition to the orders issued to the six firms, the CFPB announced that it will be studying payment system practices of Chinese tech firms in the space.

Topics Addressed

The marketing-monitoring orders are focused on the companies' consumer-to-business and/or consumer-to-consumer payment products. The topics covered in the orders include:

- Product pricing and fees;
- Intermediaries and third parties involved in the offering of the product;
- Financial information (*e.g.*, revenue obtained from the products);

[2] 12 U.S.C. § 5512(c)(4)(B)(ii)

[3] CFPB, "Statement of the Director Regarding the CFPB's Inquiry into Big Tech Payment Platforms," (Oct. 21, 2021).

- "Data harvesting," including whether and how data is aggregated and anonymized;
- Potential uses of gathered data, including to prevent fraud and to facilitate delivery of the products;
- Data retention practices;
- Monetization and selling of consumer data from the products;
- How companies have used data from the products in connection with developing, selling or marketing *other* products or services provided to consumers or commercial clients;
- User data and metrics; and
- Consumer protections, including:
  - What customers are told about their use of the products and what data is maintained;
  - Differences in data collected based on the customer's age;
  - Retention of data regarding customers race and ethnicity; and
  - Billing error notices.

Responses to the marketing monitoring orders are due on December 15, 2021, although companies may potentially negotiate extensions of that deadline.

Key Takeaways

The CFPB's market-monitoring orders suggest that payments processes, particularly at large technology firms, will be subject to substantial scrutiny going forward. The use of consumer data, including privacy, consumer control and aggregation, were also areas of focus in the CFPB's November 2020 request for information regarding consumer access to financial records.[4] These actions suggest that the CFPB is likely to issue rules or other regulations in 2022 regarding the safeguarding and use of consumer data.

Return to Table of Contents

Rulings in the UK and Australia Suggest Surveillance Cameras and Collection of Customer Photos May Implicate Privacy Laws

Two October 2021 decisions in the United Kingdom and Australia highlight how the use of video cameras and collection of facial images may violate privacy laws.

The month of October saw two separate rulings in which the use of image capturing technology were found to violate applicable privacy laws. In the first ruling, a court held that the use of a video doorbell and security camera system that captured images of a neighbor's home violated the U.K.'s version of the General Data Protection Regulation (U.K. GDPR). In the second decision, an Australian privacy regulator concluded that a company's use of a tablet with a built-in camera to capture facial images of consumers that were taking a customer survey violated the country's privacy laws. Together, these cases serve as a reminder that the use of new technologies in traditional applications can raise unexpected privacy issues.

UK: Home Surveillance

In early October 2021, a U.K. judge ruled that a homeowner who installed a "smart" video doorbell and other security cameras that captured live video of his neighbor's home violated the U.K. GDPR.[5] The homeowner had installed several motion-sensor surveillance cameras that captured both audio and video outside of his home, along with a smart doorbell device, after a reported attempted theft of his car. The security cameras had wide-angle lens cameras with motion sensors, infrared night vision, built-in microphone and speakers, and two-way audio facilities. The homeowner received alerts on his smartphone when the camera detected movement, including when his neighbor drove in and out of her parking space. When activated by motion sensors, the cameras sent 30-second video clips of the activity to the homeowner's smart devices; however, the devices could also provide video and audio feeds on demand through the homeowner's app. While the doorbell camera would be activated by the ringing of the doorbell and would view no more than someone standing on the front step immediately in front of the door, the other surveillance cameras filmed a wider field of view. The case also revealed that the smart doorbell device captured audio in a range that covered the neighbor's home and most of her garden.

The main concerns outlined in the case included the field and depth of view of the cameras; the sensitivity of the microphone and how far it could pick up sound; whether the camera and audio functions were triggered by motion or activated automatically; and how and for what purpose the data was stored. In her ruling, Judge Melissa Clark of the County Court of Oxford ruled that the images and audio files collected by the homeowner's surveillance cameras were his neighbor's personal data within the meaning of the U.K. GDPR, and thus, the homeowner must comply with the law when processing such personal data. The judge found such processing occurred when the homeowner retained surveillance images on his personal devices

[4] CFPB, "Advanced Noticed of Proposed Rulemaking, Consumer Access to Financial Records," 85 Fed. Reg. 71,003 (Nov. 6, 2020).

[5] The full decision in this case can be found here.

and sometimes shared them with other neighbors as part of a neighborhood watch group. The court also found that devices also violated the data minimization principle by capturing audio and video to a greater extent than necessary. Additionally, Ms. Clark ruled that a homeowner's right to privacy in her home, her right to leave from and return home, and her right to entertain visitors without her personal data being captured outweighed her neighbor's interest in protecting his car from theft.

As a result of the U.K. GDPR violations, the court could require the homeowner to pay a fine of up to £100,000, but it has not yet determined the amount.

Australia: Image Capture During a Survey

On October 12, 2021, the Office of the Australian Information Commission (OAIC) ruled that convenience store chain 7-Eleven violated the country's privacy laws when it collected facial images of customers who voluntarily completed in-store surveys using tablet computers without proper consent or reasonable notice.[6] The OAIC found the tablets captured facial images of customers twice: first when a person began the survey and again when the survey ended. According to the OAIC, 7-Eleven retained the facial images on an Australian server and used that information to generate algorithmic representations, known as "faceprints," which can approximate a person's age and gender. 7-Eleven stated it collected this information in order to exclude duplicative or non-genuine responses, as the faceprints were cross-referenced with all other faceprints collected from the tablets in the previous 24 hours and flagged for review if there were matches. While 7-Eleven stated the faceprints "effectively expired" after 24 hours, the company did not provide the OAIC with information on whether the faceprints were deleted.

7-Eleven claimed it provided a notice in its stores and on its website, notifying users that it may collect photographic or biometric information. However, the OAIC found this notice was not sufficient and proper consent was not obtained because 7-Eleven did not provide any information to customers about how their facial images would be used or stored and did not specify that this collection would occur via the tablets. The OAIC also concluded that the scale of the company's biometric data collection exceeded the scope of what was reasonably necessary to understand its customers' in-store experiences and that customers' rights to privacy outweighed the benefit to the business in collecting such biometric data.

In light of the privacy law violations, the OAIC ordered 7-Eleven to destroy all faceprints collected and to stop collecting facial images of its customers through voluntary surveys.

[6] The full decision can be found here.

Key Takeaways

- These two cases illustrate that as more technology becomes available for relatively common tasks, such as home security and conducting customer surveys, entities and individuals must be mindful of how their use can implicate privacy laws. These laws can be generic privacy laws, such as the U.K. GDPR, but can also be more specific to the collection of photographic or biometric information, as laws such as Illinois' Biometric Information Privacy Act, which seek to protect users' personal data.
- While the U.K. case related to an individual homeowner violating privacy laws through his use of surveillance cameras, the lessons of the ruling can be applied to other entities using similar security measures. Companies using surveillance devices that capture audio and video should take appropriate steps to avoid similar liability, making sure to be mindful of what information these systems capture beyond the immediate environs. The 7-Eleven case illuminates the importance of ensuring proper notice and consent before the collection of sensitive personal data. Companies should note that statements made online in a privacy policy or displayed in brick-and-mortar stores may not be sufficient as the basis for consent.

Return to Table of Contents

Judicial Panel on Multidistrict Litigation Denies Centralization for Putative Class Actions Arising From Insurer's Data Breach

The Judicial Panel on Multidistrict Litigation (JPML) recently held that five proposed class actions against Geico[7] stemming from a data breach should not be centralized, reasoning that centralization is not necessary and that informal coordination is more appropriate given the small number of cases.

On October 4, 2021, the JPML denied Geico's request to centralize five proposed class action lawsuits arising from a data breach suffered by Geico.[8] The JPML reasoned that centralization was not necessary to further the efficiency of the litigation or for the convenience of those involved, noting that informal coordination is feasible and appropriate given the small number of cases.

[7] Government Employees Insurance Company, GEICO Indemnity Company, GEICO Casualty Company and GEICO General Insurance Company.

[8] *In re: Geico Customer Data Security Breach Litigation*, MDL No. 3013, Dot No. 33 (J.P.M.L Oct. 4, 2021).

Geico's Data Breach and the Proposed Class Actions

On April 15, 2021, Geico filed a data breach notification with the California Office of the Attorney General, disclosing that the company had suffered a data security breach earlier in the year. According to Geico, hackers bypassed security and entered the company's online sales systems, gaining access to customers' driver's license numbers between January and March 2021. Geico specified in the notification that the hackers might have planned to use this customer information in an attempt to fraudulently apply for unemployment benefits.

The data breach incident prompted the filing of five putative class actions — three of which are pending in the Eastern District of New York, with one each pending in the District of Maryland and the Southern District of California. The actions share common questions of fact, such as how the hackers were able to gain access to Geico's systems, the security measures Geico had in place at the time and the protective measures taken once Geico was alerted of the breach.

Geico's Bid to Centralize the Putative Class Actions

On June 29, 2021, Geico moved pursuant to 28 U.S.C. Section 1407 and the Rules of Procedure of the JPML to transfer the five putative class actions to the Eastern District of New York (where the majority of the lawsuits were filed) or, in the alternative, the District of Maryland (where Geico is headquartered) for consolidation or coordination of pretrial proceedings. The plaintiffs in four of the five putative class actions supported Geico's motion. However, the plaintiffs in the California putative class action opposed centralization of the lawsuits, arguing that their case involves a unique state law claim under the California Consumer Privacy Act (CCPA), and other states do not have a similarly applicable law.

The JPML's Decision

On October 4, 2021, the JPML issued an order denying Geico's motion to transfer, concluding that centralization was not necessary for the convenience of the parties and witnesses or to further the just and efficient conduct of the litigation.

While the JPML acknowledged that the actions "share common questions of fact," the judicial body observed that there were only five actions pending, three of which were already pending in the same district before the same judge, with no potentially related actions brought to the JPML's attention. Under these circumstances, the JPML explained, "the proponent of centralization bears a heavier burden to demonstrate that centralization is appropriate," and "[Geico] has failed to meet that burden here." The JPML also emphasized that "'centralization under Section 1407 should be the last solution after considered review of all other options.'" Here, "informal coordination among the small number of parties and involved courts appears eminently feasible." The panel of seven judges that make up the JPML therefore proceeded to deny Geico's motion.

Key Takeaways

While the California-based proposed class focused on the relevant state claims that make their case unique, the JPML's order did not speak to these issues. Instead, the JPML focused entirely on the number of actions and parties, and the availability of alternative means of coordination. This decision therefore may be helpful for parties seeking to avoid centralization in future cases where there are a minimal number of actions subject to centralization. The JPML also observed that three of the five cases were in the same district, opening the door for parties to argue that even in larger-scale litigations, centralization might not appropriate if the majority of cases are already pending in one venue.

Return to Table of Contents

Two States Amend Laws to Strengthen Genetic Privacy

California and Florida have both taken steps to protect the privacy of genetic information, signifying the growing push to safeguard personal health and related data.

In California, Gov. Gavin Newsom signed the Genetic Information Privacy Act (GIPA) into law, codifying the protection of the privacy and security of genetic data processed by direct-to-consumer genetic testing companies (DTC companies). Also this month, the state of Florida's Protecting DNA Privacy Act went into effect, creating four new crimes for the unlawful use of a state resident's DNA. These two laws reflect a growing focus on the potential for misuse of genetic information and are outlined in further detail below.

California's Genetic Information Privacy Act

On October 6, 2021, Gov. Newsom signed the GIPA into law, imposing privacy requirements on DTC companies.[9] The governor had previously vetoed a similar law in 2020. Effective January 1, 2022, DTC companies will have to comply with various regulations related to their handling of consumers' genetic data or face civil penalties ranging from $1,000 to $10,000 per

[9] The text of the law is available here.

violation (plus court costs). The GIPA is similar in some ways to the CCPA, and requires DTC companies to:

- provide consumers certain notices explaining the individual DTC company's privacy practices;
- obtain consumers' express consent for the collection, use and disclosure of their genetic data;
- contractually restrict service providers' use of consumers' genetic data; and
- develop procedures and practices enabling consumers to exercise privacy rights with respect to their genetic data (*e.g.*, data access, data deletion, biological sample destruction and protection against discrimination for exercising privacy rights).

The GIPA also includes obligations beyond those in the CCPA, requiring companies to:

- implement and maintain reasonable security procedures and practices to protect consumers' genetic data; and
- refrain from giving consumers' genetic data to any entity (1) that is responsible for administering or making decisions regarding health insurance, life insurance, long-term care insurance, disability insurance or employment; or (2) that provides advice to an entity that is responsible for performing these functions.

Certain exemptions apply to the GIPA, including a general exemption for covered entities or business associates governed by the Health Information Portability and Accountability Act (HIPAA), as well as one regarding the use of genetic data used by an employer in order to comply with applicable law.

The GIPA also includes an exemption for deidentified information, which may be familiar to those experienced with HIPAA, but the GIPA does not adopt the HIPAA standard for deidentification. Instead, it imposes a more stringent standard for what qualifies as deidentified information and imposes a set of CCPA-like procedural requirements that companies must meet in order to enjoy the benefit of the GIPA exemption. Specifically, in order to qualify as deidentified, the information itself must not be able to be used to infer information about, or otherwise be linked to, a particular individual. Once the information meets that standard, DTC companies must also ensure all of the following with respect to the deidentified information:

- take reasonable measures to ensure that the information cannot be associated with a consumer or household;
- publicly commit to maintain and use the information only in deidentified form and not to attempt to reidentify the information (other than to test the effectiveness of its deidentification process); and
- contractually obligate any recipients of the information to take reasonable measures to ensure that the information cannot be associated with a consumer or household and commit to maintain and use the information only in deidentified form.

As with the CCPA, there is no private right of action to enforce the GIPA. Instead, enforcement is left with to the state's attorney general.

Florida's Protecting DNA Privacy Act

On October 1, 2021, Florida's Protecting DNA Privacy Act (DPA) went into effect.[10] The law criminalizes the collection, retention, analysis and disclosure of a Florida resident's DNA sample or DNA analysis without express consent, establishing both misdemeanor and felony crimes related to these actions.

Under the DPA, a person is guilty of a misdemeanor if, without consent, they willfully collect or retain an individual's DNA sample with the intent to perform a DNA analysis. A person is guilty of either a second-degree or third-degree felony (depending on the specific act) if, without consent, they either:

- willfully analyze, submit for analysis, or procure the analysis of another individual's DNA sample; or
- sell or otherwise transfer an individual's DNA sample or DNA analysis results to a third party, even if the original sample was collected with consent.

Prior to the DPA, DNA analysis without consent constituted a first-degree misdemeanor. Like the GIPA, the DPA provides for certain exemptions where collecting and analyzing DNA samples without consent is not a criminal offense, including for purposes of criminal investigations or prosecutions; compliance with federal law; a designated newborn screening program; certain paternity determinations under relevant laws; and certain research, including utilizing certain deidentified information, under applicable federal regulations. The DPA also states that the genetic information of the person from whom it is extracted is the "exclusive property" of that person to control.

Penalties under the DPA can include 15 years in prison and a $10,000 fine.

Key Takeaways

The GIPA and the DPA highlight the growing desire of governments to protect the privacy of genetic information — in these cases by regulating companies trading in health, medical, genetic or biometric data. As sensitivity around the mass collection and disclosure of personal health information looms

[10] A copy of the law can be found here.

large in the era of COVID-19, genetic screening for certain diseases and consumer use of genetic information for genealogical purposes, stakeholders in this space should expect to see continued focus on the management of this information.

Return to Table of Contents

UK Government Launches National Artificial Intelligence Strategy

The U.K. government has published a document outlining its approach to encouraging artificial intelligence growth and innovation in the country.

On September 22, 2021, the U.K. government published its National Artificial Intelligence Strategy (the National AI Strategy),[11] a 10-year plan that outlines the goal of making the U.K. a "global AI superpower" with the intention of building the most "pro-innovation regulatory environment in the world." The National AI Strategy also seeks to highlight the socioeconomic benefits of AI, and aims to develop a regulatory framework that fosters economic growth.

Background

The U.K. government regards the National AI Strategy as the next significant step in building upon Britain's recent successes in the AI field. It follows the 2017 Industrial Strategy, which laid down the government's vision to transition the U.K. into a global center for AI innovation, as well as the government's 2018 AI Sector Deal, which included an announcement of a £1 billion package of investment to improve the U.K.'s global standing as a leader in developing AI technologies.

The Three Pillars

The National AI Strategy involves three core pillars:

- Invest and plan for the long-term needs of the AI ecosystem to continue the U.K.'s leadership as a science and AI superpower. The government plans to, inter alia:
  - introduce new visa regimes and revise immigration rules to enable the U.K. to attract AI talent from around the world;
  - launch a joint office for AI with the U.K. Research and Innovation Body with the aim of creating and developing new AI technologies; and
  - increase AI-specific education in schools, higher education providers and businesses through AI skills "bootcamps."
- Support the transition to an AI-enabled economy, capturing the benefits of innovation in the U.K. and ensuring AI benefits all sectors and regions. This pillar involves efforts on multiple fronts, including:
  - The government intends to launch a consultation on copyrights and patents for AI through the U.K. Intellectual Property Office with the aim of simplifying the commercialization of AI technologies by facilitating the creation of intellectual property rights in AI technologies for businesses.
  - The government reiterated that it is focused on improving awareness of the societal benefits of AI investment, particularly in the fields of public health and defense. To this end, the government is set to publish an AI strategy for defense in the next three months and begin engagement on a draft national strategy for AI-driven technologies in health and social care.
  - The National AI Strategy also supports proposals made by the government in its consultation on reform of the U.K. GDPR, which was published on September 10, 2021. In the consultation, the government set out plans to review Article 22 of the U.K. GDPR, which grants data subjects the right not to be subject to a decision based solely on automated processing (including profiling), which accordingly has an impact on the extent to which organizations can use AI to automate routine processes. A review of the interaction between AI and Article 22 of the U.K. GDPR was welcomed by the U.K.'s Information Commissioner's Office (ICO) in its response to the consultation published on October 7, 2021.[12]
- Ensure the U.K. gets the national and international governance of AI technologies correct in order to encourage innovation, investment, and protect the public and the U.K.'s fundamental values.
  - In particular, the government plans — among other things — to pilot an "AI Standards Hub" and "Standards Engagement Toolkit" to address Britain's engagement with global AI standardization. It also plans to revisit whether AI regulation in the U.K. is best conducted via the current sector-by-sector approach. The government noted certain advantages of this approach, including the fact that individual regulators (such as the ICO), are typically best placed to legislate on industry-specific complexities of AI. However, the government also accepted that a sector-by-sector approach can create inconsistencies across regulatory sectors and risk uncertainty caused by potential overlap between regulatory mandates.

[11] The National AI Strategy is available here.

[12] The consultation was covered in our September 2021 *Privacy & Cybersecurity Update*.

Next Steps

In early 2022, the government plans to issue a white paper outlining its position on the potential risks and harms posed by AI technologies and its proposal to address them. This white paper will, among other matters, detail the government's recommendations for how to regulate the development and use of AI. The white paper, as well as the strategies for using AI in defense and in the health and social case fields described above, will further elaborate on the government's recommendations for encouraging AI innovation and deployment in key sectors, while seeking to address the risks that deployment may raise.

Key Takeaways

The release of the U.K. government's National AI Strategy represents the beginning of a significant push to use the tools at the government's disposal to promote the development of AI in Britain. Together with the white paper expected in early 2022, the Strategy also reflects how policymakers are struggling with how to regulate AI and its use, particularly in light of the U.K. GDPR's requirements on notice of automated decision-making. Companies engaged in AI development or that use AI in their businesses should pay close attention to the government's efforts in this area.

Return to able 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