Skadden

The Distributed Ledger

Blockchain, Digital Assets and Smart Contracts

SEC Launches FinHub to Liaise With FinTech Startups

On October 18, 2018, the U.S. Securities and Exchange Commission (SEC) announced the launch of a new division, the Strategic Hub for Innovation and Financial Technology (FinHub), which is intended to increase its collaboration with fintech developers, including those behind initial coin offerings (ICOs). FinHub is designed to "provide a clear path for entrepreneurs, developers, and their advisors to engage with SEC staff, seek input, and test ideas," according to its head, Valerie Szczepanik, the SEC's senior adviser for digital assets and innovation and associate director in the Division of Corporation Finance.

Following the announcement, SEC Chairman Jay Clayton stated, "FinHub provides a central point of focus for our efforts to monitor and engage on innovations in the securities markets that hold promise, but which also require a flexible, prompt regulatory response to execute our mission."

Chairman Clayton's statement is in line with some of his previous comments regarding SEC regulation in the fintech startup world and of ICOs, and we view it as an encouraging sign that the SEC is staying consistent with its current trend of seeking more collaboration between developers and regulators to responsibly grow the industry. While the SEC has also recently stepped up its enforcement of ICOs and their developers,[1] FinHub is proof of the SEC's goal of pairing that enforcement with engagement that should enable developers to more easily navigate the regulatory landscape.

SEC Director Promises ICO Guidance

The U.S. Securities and Exchange Commission's (SEC) director of Corporation Finance, William Hinman, announced on November 5, 2018, that the SEC will release "plain English" guidance to help developers to determine whether their cryptocurrency and token offerings constitute the offer and sale of securities under the federal securities laws. Directly referring to his previous comments at the Yahoo Finance All Markets Summit,[2] Director Hinman stated that the SEC "will be putting out more guidance, the

[1] *See* Skadden client alerts "The Ever-Evolving Cryptocurrency Legal Landscape" (June 19, 2018), "Rise of Blockchain and ICOs Brings Regulatory Scrutiny" (Jan. 23, 2018) and "SEC Issues Guidance on Regulation of Initial Coin Offerings," (Aug. 1, 2017).

[2] William Hinman, "Digital Asset Transactions: When Howey Met Gary (Plastic)" (June 14, 2018), https://www.sec.gov/news/speech/speech-hinman-061418 (last visited Nov. 6, 2018).

idea is a plain English instrument that people can look at, and they'll bring together sort of my Howey-meets-Gary speech and that analysis." He explained that the goal is to enable developers to "look at that guidance and ... be able to sort things out."

Director Hinman's public comments are consistent with the SEC's recent efforts to encourage engagement and collaboration with developers regarding their blockchain-related projects rather than emphasizing enforcement actions, as demonstrated by the agency's launch of FinHub.

EU Begins to Weigh in on Application of GDPR to Blockchain Technology

Regulators across a wide range of areas have struggled with how to apply existing legal structures to the decentralized paradigm of blockchain technology. A prime example of this tension has been the application of the EU General Data Protection Regulation[3] (GDPR), which went into effect in May 2018, to this relatively nascent technology. Although blockchain technology offers the potential to satisfy a key goal of the GDPR — namely, to bolster individuals' rights regarding their own personal data — it remains unclear how to apply certain fundamental GDPR provisions when data is stored or processed through a decentralized blockchain. Indeed, many have asserted that blockchain technology is simply incompatible with the GDPR.

Recent developments show that EU regulators are starting to consider how these tensions might be resolved. The French Data Protection Supervisory Authority (CNIL) recently published its initial thoughts and practical recommendations on this matter, becoming the first data protection authority to provide preliminary guidance on this matter (CNIL Report).[4] In addition, the EU Blockchain Observatory and Forum, which was created as a European Parliament pilot project and is run under the aegis of the European Commission's Directorate General for Communications Networks, Content and Technology, recently released a thorough analysis of the current tension points between blockchain technology and the GDPR, and offered proposals on how some of these may be resolved (Observatory Report).[5] Finally, in its recent Blockchain Resolution, the EU Parliament acknowledged that it is of the "utmost importance" that compliance with the GDPR is ensured, calling on the European Data Protection Board (EDPD) to provide further guidance.[6]

Main Themes of the Reports

Both the CNIL Report and the Observatory Report echo a widely held sentiment that while blockchain technology offers unprecedented opportunities, developers need to consider whether, in light of the GDPR and data protection issues, it is the most appropriate technology to use when handling personal data. The Observatory Report further notes that GDPR compliance is not about blockchain technology per se, but rather how that technology is used: "[T]here is no such thing as GDPR-compliant blockchain technology. There are only GDPR-compliant use cases and applications."

Both reports stress that where blockchain technology is used, GDPR compliance needs to be integrated from the outset at the design and implementation stages, and that actors should store data "off-chain" whenever feasible and maximize the use of data obfuscation, encryption and aggregation techniques. The Observatory Report also makes the point that the burden in this area is not solely on the developers, as the regulators themselves need to deeply understand the technology and the impact of any guidance they may issue.

The Observatory Report also returns a few times to the important distinction between public, permissioned blockchains, in which anyone can participate as a "validating node" (to validate the blockchain's transactions) or a "participating node" (to store or add data to the chain), and private, permissioned blockchains, in which the validating nodes and participating nodes must be approved by a central actor or consortium (*e.g.*, a blockchain created by a group of banks to transact with one another). GDPR compliance, in many cases, will be easier where the blockchain is private and permissioned, since it is easier to identity the key actors and data protection rules can therefore more easily be applied.

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and the free movement of such data.

[4] Commission Nationale de L'informatique et des Libertés Report, *Blockchain: Premiers éléments d'analyse de la CNIL*: 2018.

[5] The European Union Blockchain Observatory and Forum Thematic Report, *Blockchain and the GDPR*: 2018.

[6] Resolution of the European Parliament of 3 October 2018 on distributed ledger technologies and blockchains: building trust with disintermediation (2017/2772(RSP)).

We set forth below the key issues addressed by the CNIL Report and the Observatory Report.

Identifying the 'Data Controller' and 'Data Processor'

In general, the GDPR effectuates its data privacy protections by imposing obligations on the entity that determines the purpose and means of processing personal data (the "data controller") and the entity that processes data at the direction of the data controller (the "data processor"). In almost every case of data collection and usage, it is relatively easy to identify these parties. However, for many types of decentralized blockchains, where multiple nodes all have copies of, and simultaneously update, the data ledger, and where no one entity "controls" the blockchain or its data, it becomes far less obvious which party must satisfy the GDPR obligations. Some pundits have opined that every node on a blockchain is both a data controller and a data processor, while others have argue that there are no data controllers or processors on a blockchain.

According to the Observatory Report, the answer to this issue may vary depending on the type of blockchain being used. For example, in private, permissioned blockchains (*e.g.*, a bank consortium), where each participant must be pre-approved and control is more centralized, it should be easier to identify the data controller or joint controller roles. In the case of public, permissionless blockchains, the answer is less clear, and as the Observatory Report notes, has not yet been resolved by data protection authorities or the EDPB. While the Observatory Report does not recommend who should hold this role, it runs through the potential parties who might be so designated, such as the protocol developers, validating nodes, network users and publishers of the underlying smart contracts. Ultimately, the Observatory Report concludes that this will likely need to be resolved on a case-by-case basis.

The CNIL Report provides some additional guidance on this issue, but not in the difficult area of public, permissionless blockchains. Where the blockchain is operated by a consortium, the CNIL Report has recommended that the members identify the data controller as early as possible in a project, and that if they fail to do so, they will all be deemed joint controllers.[7] With respect to blockchain nodes that have permission to write data to the chain (assuming it has been validated), the CNIL Report proposes that such nodes be deemed data controllers where (i) such participating node is an individual and the data processing is linked to a professional or commercial activity (it is not personal), and (ii) the participant is a corporate entity and writes personal data onto the blockchain.

With respect to identifying data processors, the CNIL Report considers the role of the smart contract developers (where the smart contract is processing personal data on behalf of the controller) and the validating nodes (miners), but concedes that designating miners as data processors may not be realistic, since they are not going to execute data processing agreements as required under Article 28 of the GDPR. The CNIL concludes by simply asking stakeholders to be creative and seek innovate solutions so as to comply with the GDPR.

We note that the CNIL Report's view of "smart contract developer as data processor" may be misplaced, given that in many cases developers simply create template contracts that are used by others. In such cases, the developer is no more a "processor" than a company licensing out database software that others can use.

Determining Whether Data Is Anonymized

Although a cornerstone of blockchain technology is transparency, blockchains rely in great part on hashing and other cryptographic functions to cloak and represent specific data sets. Since the GDPR does not apply to personal data that has been anonymized, the question is whether hashing and other encryption techniques used on a blockchain render the data "anonymous" for GDPR purposes. The issue is challenging because the GDPR defines anonymization narrowly, requiring that it is not possible to reverse the encryption process and recreate the original data (a "reversal risk"), nor to link the encrypted data to an individual by studying usage patterns or combining it with other data (a "linkability risk").

The view of the Observatory Report is that public keys on a blockchain are not anonymous, given that there is a linkability risk by tracing multiple transactions, but notes that certain obfuscation techniques, such as ring signatures, may on a case-by-case basis satisfy the GDPR anonymization requirement. Similarly, encrypted data is likely not anonymous, given the reversibility risk arising from the existence of a decryption key and the fact that, as cryptography evolves, new decryption techniques may be developed.

[7] The CNIL did not address "private" blockchains where a single entity controls who can join the network and who can serve a validation role in the consensus process, since in these cases, the role of the data controller is clear.

Hashing presents the greatest challenge when seeking to apply the GDPR to blockchain technology, and as the Observatory Report notes, does not lend itself to easy answers, given the various types of "hashing" that exist. In general, "hashing" is the process of running text (of any length) through a program that generates a unique, fixed-length string of characters. In some cases, hashed data could be reversed if the original data size is known and short (*e.g.*, a national identification number). In other cases, hashed data might be linkable (*e.g.*, where the hash is of a wallet address that is used repeatedly). Therefore, as with many other areas relating to the intersection of GDPR and blockchain technology, the Observatory Report concludes that whether data has been sufficiently anonymized must be analyzed on a case-by-case basis.

Rights of the Data Subject

The difficulty of identifying the data controller also impacts the exercise of data subjects' rights enshrined in the GDPR. The Observatory Report and the CNIL each touch on certain of these issues.

Lawful Processing

Under the GDPR, data can only be processed if the data controller can satisfy one of the six permissible legal bases for doing so. In many cases, these bases presume that there is a central entity that can be identified as the data controller. For example, a data controller can rely on "consent" as the basis for lawfully processing data, but only if that consent is specific and unambiguous. As the Observatory Report notes, consent may be difficult to establish in a permissionless, public network.

Data Minimization

The GDPR requires that data controllers ensure that data that is collected is adequate, relevant and limited to the purpose for which it is collected and processed. The CNIL Report recognizes that data that identifies nodes on a blockchain (such as a public key) is necessary and likely has to be permanently retained, since the blockchain depends on that permanence. Other data that is subject to the GDPR should, according to the CNIL Report, be stored off chain, with information that proves the validity of that data stored on chain. For example, a hash of personal information might be stored on chain so that a user knows that off-chain information has not been tampered with. However, the CNIL Report also indicates that where it is justified for the purpose of the processing, and the residual risks are acceptable (based on a privacy impact assessment), data could be stored on a blockchain with a hash function, without a key, or if that is not an option, in clear text form.

The Data Subject's Right to Access, Erasure, Portability and Rectification

The GDPR provides data subjects with a series of important rights, including access to their data (right of access), the right to ensure their data is accurate and to require corrections when it is not (right to rectification), the right to obtain their data and reuse it for their own purposes or to transmit it to another data controller (right of portability), and a right in certain cases to have their data deleted (the right to erasure, also known as the "right to be forgotten"). A central benefit of blockchain technology, however, is "immutability" (*i.e.*, once data is stored on a blockchain, it cannot be erased or modified). This allows participants in the decentralized chain to trust that data has not been tampered with. The Observatory Report notes that the data subject's ability to exercise certain of the GDPR rights noted above can clash with blockchain technology if a data controller cannot readily be identified. Moreover, given the immutability of blockchains, even if the relevant controller could be identified, complete deletion of personal data is not technically feasible. The Observatory Report notes that these are issues that will need to be resolved. The CNIL Report focusses almost exclusively on the right of erasure. While not providing a definitive solution, it suggests that encryption coupled with the destruction of the encryption key could make the data permanently unavailable and hence possibly satisfy the right to erasure requirement, particularly since the GDPR does not define the notion of "erasure."

Smart Contracts and Automated Processing

Under the GDPR, data subjects have the right to inquire whether their data is being used for automated decision making (*e.g.*, whether decisions about whether to extend credit are being made through automated processing). If such processing takes place, an individual can challenge the resulting decision or ask for human intervention. The Observatory Report notes that since smart contracts are a form of automated processing, one might argue that any smart contract-enabled decision would trigger this right. However, once humans can be required to intervene in smart contract processes, the value of this technology diminishes greatly. Although the Observatory Report acknowledges that smart contract "profiling" does not yet exist, it will be an important area to watch.

Transborder Data Flows

Another tension point highlighted by the Observatory Report is the restriction the GDPR imposes on transfers of personal data to countries outside of the European Economic Area (EEA) that do not ensure an adequate level of protection in line with GDPR requirements. For transfers to countries that do not satisfy this standard, alternatives must be put in place, such as implementing specified contractual measures between the data exporter and data importer. The Observatory Report notes that the global scope of blockchains, coupled with the lack of restriction on who can host a node in public, permissionless networks, makes these transborder requirements extremely difficult to administer. The CNIL Report did not address this issue.

Security

The CNIL Report offers a number of suggestions to satisfy the data security requirements under the GDPR. These include setting a minimum number miners to avoid collusion attacks, and implementing organizational and technological safeguards that would mitigate the impact of an algorithm failure on the security of the network.

Development Principles for Blockchain Innovators

The Observatory Report concludes with four principles that blockchain developers should consider in connection with building GDPR-compliant applications and protocols:

- Consider how user value is created and data is used to determine if a blockchain solution is really necessary;
- Avoid storing personal data on chain (even if encrypted), but instead use blockchain networks to store immutable proof that data exists;
- Collect personal data off chain or on private, permissioned blockchains; and
- Be clear and transparent with users.

Key Takeaways

The CNIL Report and the Obervatory Report highlight that the application of the GDPR to blockchain technology is more nuanced than a simple reaction that they are incompatible. For the near-term, applying the GDPR to blockchain technology will require a case-by-case and pragmatic approach. Interestingly, while blockchain technology is at its earliest stages, the same argument can be made regarding the GDPR, which despite going into effect in May 2018, is still being clarified through guidance. Companies subject to the GDPR also await publication of a comprehensive set of official guidelines from the EDPB. However, for blockchain developers, the key takeaway from the CNIL report and the Obervatory Report is that they cannot assume that GDPR does not apply in the blockchain context, but instead build protocols and solutions that are in compliance.

CFTC Commissioner Discusses Regulatory Framework for Blockchain Smart Contracts

On October 16, 2018, CFTC Commissioner Brian Quintenz spoke at the 38th Annual GITEX Technology Week Conference in Dubai about how the existing Commodity Exchange Act (CEA) regulatory framework may apply to emerging smart-contract applications on the blockchain. In particular, Quintenz addressed how the CFTC may approach enforcement if it determines that smart contracts programmed on the blockchain fit the definition or facilitate the trading of futures, swaps, options or event contracts. Quintenz's speech emphasized the challenge of adapting a pre-existing regulatory scheme to new technologies — in this case, a technology whose decentralized structure is fundamentally different from the structure of intermediation on which the CEA is based.

Quintenz's remarks are notable for providing preliminary views on how he would approach questions that are on the minds of many market participants regarding how the CFTC will address novel issues raised by the products of blockchain technology. Quintenz focused on smart contracts that could fall within CFTC jurisdiction, either because they resemble products that the CFTC regulates or because they offer functionality that would permit or facilitate trading of such products. He acknowledged that many of these contracts may not be in compliance with the CFTC statutes and rules and, assuming that were the case, addressed issues relating to who would be assigned legal responsibility for smart contract noncompliance. Quintenz suggested that while developers of the underlying blockchain, miners and others play a role in the use of smart contracts, it is the smart

contract code developers who could be held accountable, at least where they "could reasonably foresee, at the time they created the code, that it would likely be used by U.S. persons in a manner violative of CFTC regulations."[8]

If the CFTC were to adopt such a standard, smart contract code developers would need to be comfortable that the code they are building will not be likely to facilitate activity that violates the CEA, such as trading of off-exchange swaps between retail customers.[9] Given that these are unchartered waters, it also would be prudent for smart contract developers to reach out to the CFTC before rolling out their product. Quintenz encouraged precisely such engagement, observing that he "would much rather pursue engagement than enforcement — but in the absence of engagement, enforcement is our only option."[10] Quintenz suggested in particular engagement with the CFTC's LabCFTC, a group that Chairman J. Christopher Giancarlo established to promote dialog between the agency and the fintech community for their mutual benefit. Given the CFTC's support for innovation, Quintenz noted that such engagement could spur "the Commission to rethink its existing regulations or provide regulatory relief — both courses of action that I think would be appropriate depending upon the technology in question."[11]

To date, the CFTC has exercised its enforcement authority in the blockchain and cryptocurrency space in two primary ways: (i) policing fraud in the sale of cryptocurrency to retail purchasers,[12] and (ii) ensuring that leveraged spot transactions with retail investors are not illegal futures contracts.[13] However, as blockchain innovators develop applications that facilitate the execution of contracts falling under CFTC jurisdiction or create platforms on which derivatives will be traded, both the developers and the CFTC will need to consider whether and to what extent CEA provisions and CFTC rules apply to these activities.

Financial Action Task Force Updates Recommendations Related to the Regulation of Virtual Assets

On October 19, 2018, the Financial Action Task Force (FATF) released updated recommendations related to the regulation of "virtual assets" for anti-money laundering/countering terrorist financing (AML/CTF) purposes. While not legally binding, countries often look to the FATF Recommendations[14] in shaping their domestic laws regarding AML/CTF. The Recommendations are likely to continue to evolve as distributed ledger and blockchain technologies, and their various applications, develop and mature.

The FATF first issued guidance on mitigating the AML/CTF risks of virtual currencies in 2014 and 2015.[15] FATF has indicated that, since that time, governments and the private sector have sought additional clarity from the FATF regarding activities to which the FATF virtual currency standards apply.[16] In response, the FATF updated Recommendation 15, titled "New Technologies," in which the FATF advises that countries should ensure that "virtual asset service providers" are regulated for AML/CFT purposes; licensed or registered; and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the Recommendations.

A "virtual asset" is defined by FATF as "a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes." Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the Recommendations.

[8] Brian Quintenz, Commissioner, U.S. Commodity Futures Trading Commission, Remarks at the 38th Annual GITEX Technology Week Conference (Oct. 16, 2018), https://www.cftc.gov/PressRoom/SpeechesTestimony/opaquintenz16 (Quintenz Remarks).

[9] *See* CEA Section 2(e).

[10] Quintenz Remarks, *supra* note 1.

[11] *Id.*

[12] *See CFTC v. Kantor*, Civil Action No. 2:18-cv-2247-SJF-ARL (E.D.N.Y. May 2, 2018) (order granting preliminary injunction); *CFTC v. My Big Coin Pay, Inc. et al.*, No. 1:18-cv-10077-RWZ, Comm. Fut. L. Rep. (CCH) ¶ 34,345 (D. Mass. Sept. 26, 2018); *CFTC v. McDonnell*, No. 1:18-cv-00361-JBW-RLM , Comm. Fut. L. Rep. (CCH) ¶ 34,305 (E.D.N.Y. Aug. 23, 2018); *CFTC v. Nicholas Gelfman et al.*, No. 1:17-cv-07181-PKC (S.D.N.Y Oct. 16., 2018).

[13] *See In re BFXNA Inc. d/b/a BITFINEX*, CFTC No. 16-19, Comm. Fut. L. Rep. (CCH) ¶ 33,766 (June 2, 2016); *CFTC v. 1pool Ltd. et al.*, No. 1:18-cv-02244-TNM (D.D.C. filed Sept. 27, 2018). The CFTC did reach a settlement order with an entity that admitted to offering illegal off-exchange options on bitcoin. *See In the Matter of Coinflip, Inc., et al.*, CFTC No. 15-29, Comm. Fut. L. Rep. (CCH) ¶ 33,538 (Sept. 17, 2015).

[14] FATF, "The FATF Recommendations," updated October 2018, http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf (Recommendations).

[15] FATF, "Virtual Currencies, Key Definitions and Potential AML/CTF Risk," June 2014, http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf; FATF, "Guidance for a Risk-Based Approach, Virtual Currencies," June 2015, http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf.

[16] FATF, "Regulation of Virtual Assets," Oct. 19, 2018, http://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets.html (Oct. 2018 Announcement).

A "virtual asset service provider" is defined as any natural or legal person that "as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:

i. exchange between virtual assets and fiat currencies;

ii. exchange between one or more forms of virtual assets;

iii. transfer[17] of virtual assets;

iv. safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and

v. participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset."

The FATF notes that virtual asset service providers include "certain types of wallet providers, and providers of financial services for Initial Coin Offerings [(ICOs)]."[18] It is unclear exactly which types of wallet providers the FATF intends to capture, although the FATF may be distinguishing between custodial and noncustodial wallets. The FATF also did not elaborate on what it considers to be "financial services" for an ICO.

Aside from potential licensing and registration, the FATF recommends that jurisdictions ensure virtual asset service providers implement risk-based AML/CTF controls, including, for example, customer due diligence and ongoing monitoring, recordkeeping and reporting of suspicious transactions. Ultimately, jurisdictions have flexibility in how they regulate virtual assets, and the FATF recognizes that some jurisdictions may prohibit virtual assets altogether.[19]

In light of the rapid development of virtual assets and their applications, the FATF has stated it will continue to monitor developments and update the Recommendations accordingly. Additionally, the FATF will prepare clarification and guidance for jurisdictions in managing the AML/CTF risks of virtual assets, to include guidance on a risk-based approach to regulating virtual asset service providers, and guidance for operational and law enforcement authorities on identifying and investigating illicit activities involving virtual assets.[20]

[17] In the context of virtual assets, "transfer" means to conduct a transaction on behalf of another natural or legal person that moves a virtual asset from one virtual asset address or account to another.

[18] The October 2018 Announcement, at 2.

[19] *Id.* at 3.

[20] *Id.*

Contacts

Alexander C. Drylewski
Partner / New York
212.735.2129
alexander.drylewski@skadden.com

Ryan J. Dzierniejko
Partner / New York
212.735.3712
ryan.dzierniejko@skadden.com

Gregory A. Fernicola
Partner / New York
212.735.2918
gregory.fernicola@skadden.com

Eytan J. Fisch
Partner / Washington, D.C.
202.371.7314
eytan.fisch@skadden.com

Nathan W. Giesselman
Partner / Palo Alto
650.470.3182
nathan.giesselman@skadden.com

Alex Jupp
Partner / London
44.20.7519.7224
alex.jupp@skadden.com

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

James A. McDonald
Partner / London
44.20.7519.7183
james.mcdonald@skadden.com

Peter B. Morrison
Partner / Los Angeles
213.687.5304
peter.morrison@skadden.com

Danny Tricot
Partner / London
44.20.7519.7071
danny.tricot@skadden.com

Mark D. Young
Partner / Washington, D.C.
202.371.7680
mark.d.young@skadden.com

Jonathan Marcus
Of Counsel / Washington, D.C.
202.371.7596
jonathan.marcus@skadden.com

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

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