Holland & Knight
美国霍兰德奈特律师事务所
www.hklaw.com

CHINA PRACTICE 期刊
NEWSLETTER

SEPTEMBER - OCTOBER 2021
2021 年 9、10 月刊

Table of Contents

China Practice Newsletter

Holland & Knight is a U.S.-based global law firm committed to provide high-quality legal services to our clients. We provide legal assistance to Chinese investors and companies doing business or making investments in the United States and Latin America. We also advise and assist multinational corporations and financial institutions, trade associations, private investors and other clients in their China-related activities. With more than 1,600 professionals in 30 offices, our lawyers and professionals are experienced in all of the interdisciplinary areas necessary to guide clients through the opportunities and challenges that arise throughout the business or investment life cycles.

We assist Chinese clients and multinational clients in their China-related activities in areas such as international business, mergers and acquisitions, technology, oil and energy, healthcare, real estate, environmental law, private equity, venture capital, financial services, taxation, intellectual property, private wealth services, data privacy and cybersecurity, labor and employment, ESOPs, regulatory and government affairs, and dispute resolutions.

We invite you to read our China Practice Newsletter, in which our authors discuss pertinent Sino-American topics. We also welcome you to discuss your thoughts on this issue with our authors listed within the document.

霍兰德奈特律师事务所是一家位于美国的全球性法律事务所，我们致力于向客户提供高质量的法律服务。我们向在美国及拉丁美洲进行商业活动或投资的中国投资人及公司提供他们所需的各类法律协助。我们也向跨国公司、金融机构、贸易机构、投资人及其他客户提供他们于其与中国相关活动中所需的咨询和协助。我们在 30 个办公室的 1600 多名对各领域有经验的律师及专业人员能够协助客户处理他们在经营或投资过程中所遇到的各种机会及挑战。

我们向中国客户及从事与中国有关活动的跨国客户提供法律协助的领域包括国际商业、企业并购、科技法律、石油及能源、医疗法律、房地产、环保法律、私募基金、创投基金、金融法律服务、税务、知识产权、私人财富管理法律服务、信息隐私及网络安全、劳动及雇佣法律、员工持股计划、法令遵循及政府法规、及争议解决。

我们邀请您阅读刊载我们各作者就与中美有关的各议题所作论述的 China Practice 期刊。我们也欢迎您向本期刊的各作者提供您对各相关议题的看法。

Non-Fungible Tokens and Intellectual Property Law: Key Considerations

By Daniel J. Barsky

This article discusses some of the novel legal issues that non-fungible tokens (NFTs) raise in the area of intellectual property law, including key issues in NFT marketplace user agreements, licenses, and copyright ownership considerations. The article also provides an overview of NFT technology and discusses the major NFT marketplace types and how they function, as well as the types of works that have been minted into NFTs.

OVERVIEW OF NFT TECHNOLOGY

NFTs have existed since at least 2017 but exploded in popularity in 2021. An NFT is a unique, one-of-a-kind crypto token that is managed on a blockchain (a type of decentralized ledger that, like a bank ledger, records transactions between the various users of the blockchain). In the NFT context, the blockchain tracks and reports the ownership and transfer history of NFTs.

There is a critical difference between NFTs and the other types of tokens, such as cryptocurrency, that exist on blockchains. While traditional cryptocurrency is fungible (e.g., one bitcoin is fundamentally the same as any other bitcoin), NFTs are non-fungible. This means that each and every NFT is, in some way, different from each and every other NFT.

NFTs can exist on any blockchain that has a defined NFT standard, such as:

- Ethereum
- Flowchain
- Wax

Ethereum and its ERC-721 standard is the most common and popular.

NFTs are created in a process known as "minting" where the unique token is formed in compliance with the standards set on the blockchain used. There are various publicly available programs (such as MintBot and Enjin) that allow a user to mint an NFT. Most major NFT marketplaces also support minting, sometimes for a fee. For more information on these marketplaces, see {NFT Marketplaces} below.

NFTs contain, at a minimum:

- A unique identifier
- Metadata
- Code (also known as a smart contract) that handles properties such as transferability and ownership

Beyond these fundamentals, an NFT can be programmed in an almost limitless variety of ways, so long as it complies with the standard under which it is created. For instance, an NFT might link to a piece of art and incorporate contractual rights that provide the original artist a commission on all future sales of that piece of art.

It is equally important for practitioners to also understand what an NFT is not. NFTs are not:

- **The underlying asset itself.** Think of an NFT like a record of a deed for real property, not the real property itself. The recorded deed shows the world who owns the real property (ownership), the chain of title for the real property (transfer history), and can include additional language such as restrictions, easements, and future conveyances (akin to smart contract language). But the recorded deed is not the real property itself, just like an NFT is not the underlying asset itself.
- **Limited in number.** While NFTs are non-fungible, they are not limited in number like some cryptocurrencies, such as bitcoin. The only limits on NFT creation are the creativity of individuals and the computational limitations of a chosen blockchain.
- **Representative of a unique asset.** Each NFT itself may be unique but the underlying asset an NFT represents may not be unique. For instance, outside the technical limitations of a chosen blockchain, there is nothing to prevent an artist from creating one million NFTs representing one million copies of the same piece of art.

NFT MARKETPLACES AND HOW THEY FUNCTION

Because it would be extremely inefficient for users to find buyers and sellers of NFTs on an ad hoc basis, NFT marketplaces have become the overwhelming choice for transacting NFTs. Marketplaces are almost as diverse as NFTs themselves. They:

- Exist on different blockchains
- Can specialize in specific types of assets or be generalized
- Charge different types and amounts of fees
- Can restrict access or be open
- Have different use agreements, licenses, and rules

Marketplaces may or may not require users to create accounts to utilize the marketplace. They will, however, require a user to link his or her "blockchain wallet," which has the effect of linking the user's "blockchain account" to the marketplace. These terms are briefly discussed below, along with some examples of common NFT marketplaces.

BLOCKCHAIN ACCOUNTS

A blockchain account is essentially an address on the blockchain. It allows the blockchain ledger to associate a specific token—such as cryptocurrency, an NFT, or another type of crypto token—with a specific user.

Blockchain accounts are anonymous. For instance, an Ethereum account number starts with the prefix "0x," which is followed by a 40-digit alphanumeric code; there is no personally identifying information. Users can, however, choose to publicly associate themselves with their blockchain accounts, thereby removing anonymity.

BLOCKCHAIN WALLETS

Because the blockchain is a ledger containing millions of entries (Ethereum currently processes over one million transactions daily) between 40-digit account numbers, it is practically impossible for a user to read the blockchain. Blockchain wallets are computer code and programs that read the blockchain and display for the user the assets listed as owned by the user's blockchain account. The wallet also allows the user to conduct transactions.

Blockchain wallets do not hold any crypto tokens. Rather, if a blockchain account is like a bank account (a number on a ledger), a blockchain wallet is like a bank's application on a smartphone (giving the user access to see what is in the account).

COMMON NFT MARKETPLACES

Some common NFT marketplaces are:

- **OpenSea.** The largest NFT marketplace. It is considered a "catch all" marketplace, as it does not focus on any specific class of underlying asset.
- **Rarible.** Issues the RARI token—conveying a form of "ownership" in the platform—to active users of the platform, allowing those users to vote on certain issues. Rarible does not require a user account to utilize the marketplace. It also connects to OpenSea to broaden its reach.
- **NiftyGateway.** Markets itself as a platform for artists to sell digital works via timed "drops" that allow the creator to collect a royalty on subsequent resales of the original work.
- **NBA TopShot.** Offers officially licensed collectibles in the form of video clips, or "moments," of NBA players.
- **Digital Trading Cards.** Curates listings from OpenSea for NFTs in the collectibles and trading card spaces.

TYPES OF WORKS BEING MINTED INTO NFTS

When creating ERC-721 in 2018, the standard's creators stated that NFTs are "also known as deeds," that their rationale for creating the standard was "tracking distinguishable assets," and that future uses "include tracking real-world assets, like real-estate." While real estate transactions have not yet been turned into NFTs, a wide variety of items have been minted into NFTs, such as:

- Music
- Sneakers and shoes
- Digital art
- Physical art
- Videogame assets (such as unique swords and player skins)
- Virtual real estate

There is almost no limit as to what can be minted into an NFT. If the minimum technical requirements of the NFT standard being used are satisfied, an NFT can be minted.

KEY ISSUES IN NFT MARKETPLACE LICENSES AND USER AGREEMENTS

When counseling clients who wish to create or use an NFT marketplace, key issues to consider include:

- The relevant blockchain and associated NFT standard
- Gas fees for minting NFTs
- Transaction fees
- Setup fees

- Withdrawal fees and limitations
- Relevant rules and regulations
- Continuing royalties for creators
- Infringement and counterfeiting issues

Each is discussed below.

RELEVANT BLOCKCHAIN AND NFT STANDARD

NFT marketplaces exist on different blockchains which, in turn, have different NFT standards, which are not interchangeable. While it is possible to move an NFT from one blockchain to another, it may not necessarily be easy. Thus, when counseling clients who wish to create or use an NFT marketplace, be sure to:

- Identify the blockchain and associated NFT standard (while the Ethereum blockchain and its ERC-721 standard is the most common and popular, there are other blockchains, standards, and sub-standards, each with its own advantages and disadvantages)

- Analyze their various capabilities, restrictions, and costs, such as:
  - Transaction costs (e.g., the Bitcoin (BTC) blockchain can technically mint NFTs but transaction costs on the BTC chain create a strong financial disincentive to do so)
  - The overall number of users buying and selling NFTs on a particular blockchain (the more users, the more liquidity in a marketplace)

You should work with the client's technical team when undertaking this review, as it implicates technical requirements along with financial and legal considerations.

GAS FEES FOR MINTING NFTs

Due to the nature of current blockchains, there will always be fees (known as "gas" fees) for minting an NFT, which requires computing power and other resources such as energy. When advising clients, you must determine how much those fees are and who—the marketplace or the user—will be responsible for paying them.

Gas fees can be extremely expensive and vary widely. For instance, the gas cost to mint an NFT on Ethereum started at only a dollar or two but has since increased and can exceed hundreds of dollars per NFT. This is because pricing for gas is dynamic—the busier a blockchain is (such as Ethereum), the higher the gas fees (in other words, you need to pay more to ensure your transaction gets processed). Additionally, gas is paid in the subject blockchain's cryptocurrency, which is subject to exchange rate fluctuations against traditional currencies (such as the dollar).

Many marketplaces require the user to pay for the gas, but others (such as OpenSea) do not. This is usually done in one of two ways:

- By using a sidechain
- Lazy minting

A sidechain is a different but compatible blockchain that operates alongside of, but distinct from, the main blockchain. NFTs can be transferred from the sidechain to the main chain such that a marketplace is not forced to operate on a single chain.

There are various benefits and potential drawbacks of using a sidechain for an NFT marketplace:

- **Benefits.** Benefits of sidechains include:
  - Less traffic than the main blockchain
  - Potentially lower creation and transfer costs
  - Faster transaction processing

- **Drawbacks.** Potential drawbacks of sidechains include:
  - Additional steps that can result in friction and added complexity
  - Users utilizing multiple marketplaces may not have a seamless experience across marketplaces
  - Possible messaging and public relations issues

Lazy minting refers to the practice of not minting an NFT until there is a recorded sale, at which point the NFT is both minted and transferred. While the minting may appear to be "free," note that the cost of minting may actually be included in the transaction fee charged by the marketplace.

Also bear in mind that larger NFTs, such as those that incorporate digital artwork with large file sizes, will cost more in gas fees to mint than smaller NFTs. To reduce NFT size (and minting costs), many users mint NFTs that do not themselves contain the asset being transferred but instead contain only a link or other access right to the asset, which is stored elsewhere. However, if storing the asset outside of the NFT, you must address a host of other issues, such as:

- Where the asset is stored
- How it is stored
- How access is granted
- How security is maintained

TRANSACTION FEES

Marketplaces can elect to charge fees for transactions. Fees can be charged to the seller, the buyer, or both. Fees can be charged upfront (such as a listing fee) or taken from the proceeds of the transaction.

SETUP FEES

Some marketplaces charge a setup fee or otherwise restrict who can join the marketplace to applicants only (such as NiftyGateway and SuperRare, which require creators to apply to create NFTs on their marketplaces). These marketplaces are often trying to curate the NFTs offered for sale to increase quality and reduce potential scams.

WITHDRAWAL FEES AND LIMITATIONS

Some marketplaces (such as NBA TopShot) place restrictions on the ability of users to withdraw the proceeds

of sales of NFTs. For instance, they might charge withdrawal fees and/or restrict the timing and amounts of withdrawals.

RELEVANT RULES AND REGULATIONS

Somewhat related to withdrawal fees and withdrawal limitations are the financial regulatory and tax considerations. Many states regulate the use of cryptocurrencies. Thus, you will need to ensure you are in full compliance with the laws of every state that may affect your client. For guidance on such laws, see {Virtual Currency State Law Survey}.

For clients that are considering operating a marketplace, you will also need to review federal rules and regulations regarding transfers of money. Restrictions related to compliance need to be included in user agreements.

CONTINUING ROYALTIES FOR CREATORS

Proponents of NFTs regularly argue that continuing royalties for creators of works is a substantial benefit of NFTs. Note, however, that such royalties may not always be part of an agreement. You will need to determine whether continuing royalty payments exist and, if so:

- Who pays the royalties
- Whether a given marketplace will also take a commission on royalty payments

INFRINGEMENT AND COUNTERFEITING ISSUES

Marketplaces may be liable for indirect infringement of copyrights and trademarks. If your client is considering operating a marketplace, you will need to put in place policies and procedures for handling Digital Millennium Copyright Act (DMCA) takedown notices and other infringement allegations. These should address, among other things, whether and how user accounts and/or allegedly infringing NFTs will be restricted (such as prohibitions on displaying an infringing NFT).

For a sample policy, see {Website Copyright Policy}. For more information on the DMCA, see {DMCA Compliance and Enforcement} and {DMCA Safe Harbor for User-Generated Content}.

COPYRIGHT OWNERSHIP CONSIDERATIONS

Another key consideration is who owns the intellectual property rights for assets that are minted into NFTs. For copyrightable works, except in the case of a work made for hire, the author of a work owns the copyright. See {Copyright Fundamentals} and {Works Made for Hire}. However, because a copyright is distinct and separate from the underlying work, a sale of the work does not necessarily transfer ownership from the owner to a subsequent purchaser, absent an assignment or exclusive license. See {Transfers of Copyright Ownership} and {Assignments of Copyrights}. For instance, a person who purchases a painting would generally own the painting itself (and would be able to sell or dispose of the painting under copyright's first sale doctrine) but would not own the copyright in the painting. In this circumstance, if the purchaser minted an NFT of the painting, such act would likely constitute infringement.

Given the above, you should review an NFT to determine:

- Which copyright(s), if any, are implicated by the NFT
- Whether the party transferring the NFT owns the copyright(s)
- Whether the transferor (if the lawful owner) wishes to transfer copyright ownership with the NFT

If there are no ownership or infringement issues and the transferor wishes to transfer copyright ownership along with the NFT, they might wish to divide the various rights associated with a copyright (known as exclusive rights) and parcel them out to different holders. These rights include the rights of:

- Reproduction
- Distribution
- Adaptation
- Performance
- Display

See {Exclusive Rights of Copyright Owners}.

For example, with respect to music minted into an NFT, you could draft the associated smart contract with provisions that provide performance rights only to the purchaser of the NFT while retaining all other rights for the artist, who could then sell one of those other rights (such as the synch rights) to a different purchaser of a separate NFT. The open nature of the blockchain means it is relatively easy to track these various rights as they pass from party to party and makes tracking any associated royalty streams relatively easy compared to current standards. For more on music contracts, see {Music Contracts}.

Lastly, note that NFTs themselves are likely not copyrightable, given that U.S. law requires works of authorship to be "fixed in any tangible medium of expression" to be eligible for copyright protection. See 17 U.S.C. § 102(a). NFTs themselves are intangible and are therefore likely outside the scope of U.S. copyright law.

不可替代代币和知识产权法：主要考量因素

原文作者：**Daniel J. Barsky**

文讨论了不可替代代币（NFT）在知识产权法领域中所产生的一些新的法律问题，包括 NFT 市场用户协议、许可、及著作权的所有权方面的主要问题。本文还对 NFT 技术做了概述，并讨论了主要的 NFT 市场类型及其如何运行、以及已经铸造成 NFT 的作品的类型。

NFT 技术概述

NFT 至少从 2017 年就已经存在，但在 2021 年迅速流行。NFT 是一种独特的、独一无二的加密代币，在区块链上进行管理（一种分散的分类账，与银行分类账一样，记录区块链不同用户之间的交易）。就 NFT 而言，区块链跟踪并报告 NFT 的所有权和转让历史。

NFT 与存在于区块链上的其他类型的代币（如加密货币）之间存在着重大区别。虽然传统加密货币是可替代的（例如，一种比特币与任何其他比特币在根本上是相同的），但 NFT 是不可替代的。这意味着每个 NFT 在某种程度上都不同于其他任何及所有 NFT。

NFT 可以存在于任何具有定义 NFT 标准的区块链上，例如：

- 以太坊 (Ethereum)
- 流程链 (Flowchain)
- 蜡 (Wax)

以太坊及其 ERC-721 标准是最常见和最流行的。

NFT 是在一个称为"造币"的过程中被铸造的，而在该过程中根据所使用区块链上设定的标准铸造出独特的代币。有各种公开可用的程序（如 MintBot 和 Enjin）允许用户创建 NFT。大多数主要的 NFT 市场也支持造币，有时是收费的。有关这些市场的更多信息，请参见下文{NFT 市场}。

NFT 至少包含：

- 独特的标识符
- 元数据
- 处理转让性和所有权等财产的代码（也称为智能合同）

除了这些基本原理之外，NFT 可以以几乎无限多种方式进行编程，只要它符合创建它的标准。例如，NFT 可能会链接到一件艺术品并包含该原始艺术家未来就所有该艺术品的销售收取佣金的合同权利。

对于从业者来说，理解 NFT 不是什么也同样重要。NFT 不是：

- **标的资产本身。**将 NFT 视为不动产权状记录，而不是不动产本身。记录的权状包括显示了谁拥有不动产（所有权）、不动产的所有权链（转让历史），还可以包括其他语言，如限制规定、地役权和未来转让（类似于智能合同语言）。但记录的权状证书不是不动产本身，就像 NFT 本身不是标的资产一样。
- **数量有限。**虽然 NFT 是不可替代的，但它们的数量并不像某些加密货币（如比特币）那样有限。NFT 创建的唯一限制是个人的创造力和所选区块链的计算限制。
- **独特资产的代表。**每个 NFT 本身可能是独特的，但 NFT 所代表的基础资产可能不是独特的。例如，除了所选区块链的技术限制之外，没有任何东西可以阻止艺术家创建代表同一艺术品的一百万个复制品的 NFT。

NFT 市场及其运作方式

由于用户在个别基础上寻找 NFT 的买家和卖家效率极低，NFT 市场已成为交易 NFT 的绝大多数选择。市场几乎和 NFT 本身一样多样化。他们：

- 存在于不同的区块链上
- 可以专门从事特定类型的资产，也可以全面性的
- 收取不同类型和金额的费用
- 可以限制访问或是开放性的
- 有不同的使用协议、许可和规则

市场可能需要也可能不需要用户创建帐户来利用市场。然而，它们将要求用户链接其"区块链钱包"，这具有将用户的"区块链帐户"链接到市场的效果。下面简要讨论这些术语，以及一些常见 NFT 市场的例子。

区块链账户

区块链账户本质上是区块链上的一个地址。它允许区块链分类账将特定令牌（如加密货币、NFT 或其他类型的加密令牌）与特定用户产生连结。

区块链账户是匿名的。例如，以太坊账号以前缀"0x"开头，后跟 40 位字母数字代码；没有个人识别信息。然而，用户可以选择公开与其区块链账户的关联，从而消除其隐匿性。

区块链钱包

由于区块链是一个包含数百万条目（以太坊目前每天处理超过一百万笔交易）的 40 位账号之间的分类账，因此用户几乎不可能读取区块链。区块链钱包是读取区块链的计算机代码和程序，并向用户显示列为用户区块链帐户所有的资产。钱包还允许用户进行交易。

区块链钱包不持有任何加密代币。相反地，如果区块链账户类似于银行账户（分类账上的数字），则区块链钱包类似于智能手机上的银行应用程序（让用户可以查看账户中的内容）。

常见的 NFT 市场

一些常见的 NFT 市场包括：

- **公海 (Open Sea)。**最大的 NFT 市场。它被认为是一个"包罗万象"的市场，因为它不专注任何特定类别的基础资产。
- **稀有 (Rarible)。**向平台的活跃用户发行 RARI 代币，以传达平台中的某种形式的"所有权"，允许这些用户就某些问题进行投票。Rarible 不需要用户帐户即可使用市场。它还连接到 OpenSea 以扩大其覆盖范围。
- **NiftyGateway。**将自己营销为让让艺术家通过定时"投放"的方式销售数字作品，而使创作者可以于原创作品转售后收取权利金的平台。
- **NBATopshot。**以 NBA 球员的视频剪辑或"瞬间时刻"的形式提供官方授权的收藏品。
- **数字交易卡 (Digitable Trading Cards)。**为 OpenSea 列表中代表收藏品和交易卡的 NFT 进行策划。

被铸造成 NFT 的作品类型

在 2018 年创建 ERC-721 时，该标准的创建者表示，NFT″也称为权证″，他们创建该标准的理由是″跟踪可识别资产″，未来的用途″包括跟踪真实世界的资产，如房地产。″虽然房地产交易尚未转变为 NFT，各种各样的物品被铸造成 NFT，例如：

- 音乐
- 运动鞋和鞋子
- 数字艺术
- 实体艺术
- 视频游戏资产（如独特的剑和玩家皮肤）
- 虚拟房地产

将什么东西铸造成 NFT 几乎没有限制。如果满足所用 NFT 标准的最低技术要求，就可以铸造 NFT。

NFT 市场许可和用户协议中的关键问题

在为希望创建或使用 NFT 市场的客户提供咨询时，要考虑的关键问题包括：

- 相关区块链和相关 NFT 标准
- 铸造 NFT 的燃料费用
- 交易费用
- 安装费
- 提款费用和限制
- 相关规章制度
- 创作者的持续权利金
- 侵权和假冒问题

下文将对每一种情况进行讨论。

相关区块链和 NFT 标准

NFT 市场存在于不同的区块链上，而区块链又具有不同的 NFT 标准，这些标准是不可互换的。虽然可以将 NFT 从一个区块链移动到另一个区块链，但这并不一定容易。因此，当咨询希望创建或使用 NFT 市场的客户时，请务必：

- 确认区块链和相关 NFT 标准（以太坊区块链及其 ERC-721 标准是最常见和最流行的，但也有其他区块链、标准和子标准，各有其优缺点）
- 分析其各种能力、限制和成本，例如：
  - 交易成本（例如，比特币（BTC）区块链在技术上可以制造 NFT，但 BTC 链上的交易成本会产生强大的财务抑制因素）
  - 在特定区块链上买卖 NFT 的用户总数（用户越多，市场流动性越高）

在进行此审查时，您应与客户的技术团队合作，因为这涉及到技术要求以及财务和法律方面的考虑。

铸造 NFT 的燃料费

由于当前区块链的性质，铸造 NFT 总是需要费用（称为"燃料"费用），这需要计算能力和其他资源，如能源。在为客户提供建议时，您必须确定这些费用是多少，以及由市场或用户负责支付这些费用。

燃料费可能非常昂贵，而且差别很大。例如，在以太坊（Ethereum）上铸造一个 NFT 的燃料成本最初只有一两美元，但后来有所增加，现每个 NFT 的燃料成本可能超过数百美元。这是因为燃料的价格是动态的，区块链越繁忙（如以太坊），燃料费用就越高（换句话说，你需要支付更多以确保交易得到处理）。此外，燃料以主体区块链的加密货币支付，该加密货币受传统货币（如美元）汇率波动的影响。

许多市场要求用户支付燃料费用，但其他市场（如 OpenSea）则不要求。这通常通过以下两种方式之一完成：

- 通过使用侧链
- 惰性铸币

侧链是一个不同但兼容的区块链，与主区块链一起运行，但与主区块链不同。NFT 可以从侧链转移到主链，这样市场就不会被迫在单链上运行。

在 NFT 市场中使用侧链有各种好处和潜在缺点：

- **好处。**侧链的好处包括：
  - 流量低于主区块链
  - 创建和移转成本可能较低
  - 更快的交易处理
- **缺点。**侧链的潜在缺点包括：

- 多了些步骤可能导致摩擦和复杂性增加
- 使用多个市场的用户可能没有一个跨市场的无缝体验
- 可能的信息和公共关系问题

惰性铸币指的是在有记录的销售之前不铸造 NFT 的做法，而在销售时 NFT 既被铸造又被转让。虽然造币似乎是"免费的"，但请注意，造币成本实际上可能包含在市场收取的交易费中。

还要记住，较大的 NFT，例如那些包含大文件大小的数字艺术品的 NFT，将比较小的 NFT 花费更多的燃料费。为了减少 NFT 大小（和造币成本），许多用户造币的 NFT 本身并不包含被转让的资产，而是只包含链接或其他资产访问权，这些资产存储在别处。但是，如果将资产存储在 NFT 之外，则必须解决一系列其他问题，例如：

- 资产的存储位置
- 存储方式
- 如何授予访问权限
- 如何维护安全

交易费

市场可以选择对交易收取费用。费用可向卖方、买方或两者收取。费用可以预先收取（如上市费）或从交易收益中提取。

安装费

一些市场收取设置费或以其他方式限制只有申请人才能加入市场（如 NiftyGateway 和 SuperRare，这要求创作者申请在其市场上创建 NFT）。这些市场经常试图策划出售的 NFT，以提高质量并减少可能的欺诈事件。

提款费用和限制

一些市场（如 NBA TopShot）限制用户提取 NFT 销售收入的能力。例如，他们可能收取提款费和/或限制提款的时间和金额。

相关规章制度

与提款费用和提款限制相关的是金融监管和税务方面的考虑。许多州规范加密货币的使用。因此，您需要确保完全遵守可能影响您客户的每个州的法律。关于这类法律的指导，见{虚拟货币各州法律调查}。

对于正在考虑经营市场的客户，您还需要审查有关资金转移的联邦规则和法规。与合规性相关的限制需要包括在用户协议中。

创作者的持续权利金

NFT 的支持者经常争辩说，继续向作品的创作者支付权利金是 NFT 的一大好处。但是，请注意，此类特许权使用费可能并不总是协议的一部分。您需要确定是否存在持续的权利金支付，如果存在：

- 谁支付权利金
- 某一特定市场是否也会就权利金的付款收取佣金

侵权和假冒问题

市场可能对间接侵犯著作权和商标负有责任。如果您的客户正在考虑运营一个市场，您需要制定政策和程序来处理《数字千年著作权法》（DMCA）的撤销通知和其他侵权指控。除其他事项外，这些应解决用户帐户和/或据称侵权的 NFT 是否以及如何限制（例如禁止显示侵权的 NFT）。

有关示例策略，请参阅{网站著作权策略}。有关 DMCA 的更多信息，请参阅{DMCA 合规性和强制执行}和{DMCA 用户生成内容的安全港}。

著作权的所有权的考虑

另一个关键考虑因素是谁拥有铸造成 NFT 的资产的知识产权。对于可受著作权保护的作品，除为出租而制作的作品外，作品的作者拥有著作权。参见{著作权基础知识}和{受委托完成的作品}。然而，由于著作权与基础作品是不同且独立的，因此，如果没有转让或独家许可，作品的销售不一定会将所有权从所有者转移给后续购买者。见{著作权所有权转让}和{著作权转让}。例如，购买一幅画的人通常拥有该幅画本身（并且能够根据著作权第一出售原则出售或处置该幅画），但不会拥有该幅画的著作权。在这种情况下，如果买方铸造了该画的 NFT，则该行为可能构成侵权。

鉴于上述情况，您应该查看 NFT 以确定：

- NFT 涉及哪些著作权（如有的话）
- 转让 NFT 的一方是否拥有著作权
- 转让人（如果合法所有人）是否希望与 NFT 转让著作权的所有权

如果不存在所有权或侵权问题，且转让人希望将著作权的所有权与 NFT 一起转让，他们可能希望将与著作权相关的各种权利（称为专有权）分割，并将其分给不同的持有人。这些权利包括：

- 复制
- 发行
- 改编
- 表演
- 展示

请见{著作权所有人的专有权}。

例如，对于制作成 NFT 的音乐，您可以起草相关的智能合同，其中规定仅向 NFT 的购买者提供表演权，同时保留艺术家的所有其他权利，然后艺术家可以将这些其他权利（如同步权）中的一项出售给单独 NFT 的其他购买者。区块链的开放性意味着，当这些权利从一方传递到另一方时，追踪这些权利相对容易，与当前标准相比，追踪任何相关的特许权流相对容易。有关音乐合同的更多信息，请参见{音乐合同}。

最后，请注意，NFT 本身可能不受著作权保护，因为美国法律要求作者作品"固定在任何有形表达媒介中"，才有资格获得著作权保护。见 17 U.S.C. §102（a）。NFT 本身是无形的，因此可能超出美国著作权法的范围。

SEC Issues First-Ever Penalties for Deficient Cybersecurity Risk Controls

By Ira N. Rosner and Shardul Desai

HIGHLIGHTS

- The U.S. Securities and Exchange Commission (SEC) has launched a stunning salvo across the bows of public companies with its announcement of civil monetary penalties and a cease-and-desist order against First American Financial Corporation (FAFC) for deficient disclosure controls and procedures related to cybersecurity risks. Combined with the New York State Department of Financial Services' (NYSDFS) first-ever charges for violating the NYSDFS' Cybersecurity Regulations, FAFC has been battling regulators on multiple fronts for the same cybersecurity risk management failure.
- The warning bells and the grace periods appear to be over as the SEC and NYSDFS are now using their enforcement powers to ensure that companies implement robust cybersecurity risk management systems.
- With cyberattacks ever present and constantly evolving, it is only a matter of time that a company's cybersecurity risk management efforts and related controls, as well as corporate governance, will be exposed to regulatory scrutiny.

The U.S. Securities and Exchange Commission (SEC) has launched a stunning salvo across the bows of public companies with its announcement of civil monetary penalties and a cease-and-desist order against First American Financial Corporation (FAFC) for deficient disclosure controls and procedures related to cybersecurity risks.[1] Combined with the New York State Department of Financial Services' (NYSDFS) first-ever charges for violating the NYSDFS' Cybersecurity Regulations,[2] FAFC has been battling regulators on multiple fronts for the same cybersecurity risk management failure. In addition to the regulatory front, the NYSDFS action formed the basis of a shareholders' derivative suit against FAFC and its board of directors,[3] as well as a number of purported consumer class-action lawsuits.

The warning bells and the grace periods appear to be over as the SEC and NYSDFS are now using their enforcement powers to ensure that companies implement robust cybersecurity risk management systems.[4] With cyberattacks ever present and constantly evolving, it is only a matter of time that a company's cybersecurity risk management efforts and related controls, as well as corporate governance, will be exposed to regulatory scrutiny. To avoid substantial monetary penalties and other sanctions, companies need to develop comprehensive cybersecurity risk management standards and to test and upgrade their effectiveness regularly.

THE FAFC CASE

FAFC provides title insurance policies on residential and commercial real estate properties as well as closing and escrow services. On May 24, 2019, a cybersecurity journalist notified FAFC's investor relations personnel that its web application for sharing document images related to title and escrow transactions had a cybersecurity vulnerability that exposed sensitive personal information from more than 800 million documents from real estate transactions, including bank account numbers, mortgage and tax records, Social Security numbers, wire transactions receipts and drivers' licenses images. After FAFC shut down external access to this web application, the journalist published an article regarding the vulnerability.[5]

On May 28, 2019, the first trading day following the publication of the article, FAFC filed a Form 8-K and press release with the SEC regarding the vulnerability. Unbeknownst to the senior executives responsible for the Form 8-K disclosure, FAFC information security personnel had learned about this vulnerability months earlier, failed to remedy the problem and, most importantly in the context of the SEC enforcement action, failed to communicate the issue to senior information security management prior to the journalist's warning. Moreover, between the journalist's warning and the Form 8-K disclosure, FAFC's chief information security officer and chief information officer learned of the information security personnel's prior knowledge of the vulnerability but failed to communicate this fact to FAFC senior executives responsible for the Form 8-K disclosure (including the CEO and CFO).

SEC ENFORCEMENT ACTION: UNKNOWN CYBERSECURITY RISK IS BASIS FOR ENFORCEMENT

On June 15, 2021, the SEC announced that it had settled its enforcement action against FAFC with an agreed to cease-and-desist order and a civil monetary penalty of $487,616. The SEC found that FAFC's deficient disclosure controls and procedures related to cybersecurity risks violated Rule 13a-15(a) under the Securities Exchange Act of 1934, as amended (Exchange Act), which requires issuers registered under Section 12 of the Exchange Act to maintain disclosure controls and procedures to ensure the timely and accurate reporting of information as required by the SEC's rules and forms.

The SEC concluded that FAFC senior executives lacked information necessary to evaluate FAFC's cybersecurity responsiveness and the magnitude of the risk from the web application's vulnerability at the time they approved the Form 8-K. Despite being in the business of providing services related to real estate transactions, the SEC determined that FAFC ". . . did not have any disclosure controls and procedures related to cybersecurity, including incidents involving potential breaches of that data."[6] In announcing this settlement, the chief of the SEC Enforcement Division's Cyber Unit warned that "[i]ssuers must ensure that information important to investors is reported up the corporate ladder to those responsible for disclosures."[7]

The SEC action against FAFC is notable on a number of levels. For one, this enforcement action is the first-ever finding of a violation under Rule 13a-15(a) with respect to disclosure controls and procedures related to cybersecurity risks after nearly a decade of such warnings. In its initial 2011 guidance concerning cybersecurity risks and disclosure obligations regarding cyber incidents, the SEC warned companies to evaluate potential deficiencies in their disclosure controls and procedures with respect to cybersecurity matters.[8] In 2018, the SEC updated this guidance, in part, specifically to stress "the importance of maintaining comprehensive policies and procedures related to cybersecurity risks and incidents" in order to ensure that relevant information about cybersecurity risks and incidents is processed and reported up the corporate ladder to enable senior management to make accurate disclosures and related certifications.[9] Since the 2018 guidance, the SEC has published additional advisories concerning the development of cybersecurity risk governance standards.[10] With the FAFC action, the SEC has moved from guidance to enforcement, raising the stakes where public companies fail to implement robust cybersecurity risk management systems and related disclosure procedures.

On another level, this action continues the SEC's recent trend to deal with disclosure-related matters through rules related to internal control over financial reporting and disclosure controls and procedures.[11] By eschewing claims under securities disclosure laws, such as Sections 10 and 18 of the Exchange Act and rules thereunder, the SEC avoids the need to establish whether a disclosure was materially misleading or whether the disclosure failure involved scienter or other culpable behavior or knowledge of the persons making the disclosure. Rather, the SEC simplifies its inquiry to determine whether corporate controls and procedures alerted senior executives of particular facts and information.

Clearly, the SEC is using controls and procedures enforcement to drive cyber disclosure and to compel corporate governance standards similar to the way that executive compensation practices were influenced

by the disclosure mandates of the Compensation Disclosure and Analysis section required in proxy statements. Nevertheless, with the pervasiveness and severity of cyberattacks, it may be only a matter of time before a company's cybersecurity risk management systems fall within the regulatory (and plaintiffs' bar) crosshairs.

NYSDFS ACTIONS

The SEC is not the only agency using its regulatory powers to compel companies to develop comprehensive cybersecurity risk management systems. NYSDFS is the state government agency responsible for regulating New York financial services industries, including banks, insurance companies and mortgage loan servicers. NYSDFS issued detailed Cybersecurity Regulations, fully effective in March 2019, that set forth minimum, yet comprehensive, cybersecurity risk management systems.[12] Under the Cybersecurity Regulations, New York financial services industries must have written policies concerning 14 cybersecurity risk factors,[13] and a written incident response plan,[14] conduct annual penetration testing,[15] file annual certifications[16] and more.

On July 22, 2020, the NYSDFS announced cybersecurity charges against FAFC. These charges, which are set for a hearing later this year, carry penalties of up to $1,000 per violation, with each instance of nonpublic information in the 800 million documents exposed constituting a separate violation.[17] The charges against FAFC were the NYSDFS first-ever cybersecurity enforcement action; however, within a year, NYSDFS announced three settlements for violations of the Cybersecurity Regulations with penalties ranging from $1.5 million to $3 million.[18]

KEY TAKEAWAYS

To avoid substantial regulatory and civil claims, fines and penalties, public companies should carefully review their cybersecurity risk management systems, as well as their internal controls over financial reporting and disclosure controls and procedures related to cybersecurity risk. These controls, procedures and cyber-risk management policies should be reviewed by multifunctional teams, including personnel from information technology, internal audit, risk management and, particularly for companies operating in highly regulated industries such as financial services or that are otherwise consumer-facing, legal counsel with cyber expertise. Companies should consider enhancing written policies and procedures with respect to the various cybersecurity risk factors, establishing effective reporting structures for communicating cybersecurity vulnerabilities and cyber incidents to senior executives, developing protocols for monitoring and testing, preparing written incident response plans, and assessing various technical vulnerabilities. Moreover, because of the constantly evolving nature of cyberattacks and cybersecurity risks, regular review and testing of cybersecurity governance standards should be considered. Additionally, upon learning of cybersecurity vulnerabilities and/or cyber incidents, public companies need to quickly assess their reporting obligations to investors, the SEC and other regulatory agencies.

For more information or guidance on how to avoid an SEC enforcement action regarding cybersecurity risks, contact the authors or another member of Holland & Knight's Public Companies and Securities Team or Data Strategy, Security & Privacy Team.

Notes

[1] See SEC press release dated June 15, 2021: SEC Charges Issuer With Cybersecurity Disclosure Controls Failures and the related SEC Order.

[2] See NYSDFS press release dated July 22, 2020: Department of Financial Services Announces Cybersecurity Charge Against a Lending Title Insurance Provider for Exposing Millions of Documents With Consumer' Personal Information and the related charges.

[3] *Hollett v. Gilmore*, Case No. 1:20-cv-01620 (D. Del. Nov. 25, 2020); see also "First American hit with Dervatives Suit Over Data Breach," Rachel O'Brien, *Law 360*, Nov. 30, 2020.

[4] Indeed, as this Holland & Knight alert is being published, numerous public companies are receiving inquiries from the SEC investigating the impact of the SolarWinds cyberattack and indicating the SEC's intention to enforce failures to appropriately disclose effects of the attack.

[5] See "First American Financial Corp. Leaked Hundreds of Millions of Title Insurance Records," Brian Krebs, *Krebs On Security*, May 24, 2019.

[6] SEC Order.

[7] SEC press release dated June 15, 2021: SEC Charges Issuer With Cybersecurity Disclosure Controls Failures.

[8] See SEC Division of Corporate Finance, CF Disclosure Guidance: Topic No. 2, Oct. 13, 2011.

[9] See SEC, Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Feb. 21, 2018.

[10] See, e.g., SEC Office of Compliance and Inspection and Examination, Cybersecurity and Resiliency Observations.

[11] See, e.g., the SEC's cease-and-desist order and $20 million civil money penalty against Andeavor LLC for a failure to maintain adequate internal controls in connection with entry into a 10b5-1 plan for share repurchases.

[12] See Part 500 of Title 23 of the New York Codes, Rules and Regulations (CRR-NY).

[13] 23 CRR-NY § 500.3.

[14] 23 CRR-NY § 500.16.

[15] 23 CRR-NY § 500.5

[16] 23 CRR-NY § 500.17

[17] See NYSDFS press release dated July 22, 2020: Department of Financial Services Announces Cybersecurity Charge Against a Lending Title Insurance Provider for Exposing Millions of Documents With Consumer' Personal Information.

[18] See NYSDFS press release dated March 3, 2021, Department of Financial Services Announce Cybersecurity Settlement with Mortgage Lender; NYSDFS press release dated April 14, 2021, DFS Superintendent Lacewell Announces Cybersecurity Settlement with Licensed Insurance Company; NYSDFS press release dated May 13, 2021, DFS Superintendent Lacewell Announce Cybersecurity Settlement with . . . Life Insurance Companies.

美国证券交易委员会首次对网络安全风险控制措施不足的行为进行处罚

原文作者： Ira N. Rosner 及 Shardul Desai

重点摘要

- 美国证券交易委员会（SEC）对上市公司开启了令人震惊的打击，宣布了对第一美国金融公司（FAFC）做出民事罚款及停止令，原因是其在网络安全风险相关程序方面存有缺陷。加上纽约州金融服务部（NYSDFS）前所未有地指控其违反 NYSDFS 的网络安全法规，FAFC 一直在与监管机构就同一网络安全风险管理失败的问题进行多方面争斗。
- 由于美国证券交易委员会（SEC）和纽约州金融服务部（NYSDF）目前正在利用其执法权力来确保各公司实施稳健的网络安全风险管理系统，警告和宽限期似乎已经结束了。
- 随着网络攻击不断出现并持续演变，公司的网络安全风险管理工作和相关控制以及公司治理将受到监管审查只是迟早的问题。

美国证券交易委员会（SEC）对上市公司开启了令人震惊的打击，宣布了对第一美国金融公司（FAFC）做出民事罚款及停止令，原因是其在网络安全风险相关的披露控制和程序方面存有缺陷。[1]加上纽约州金融服务部（NYSDFS）前所未有地指控其违反 NYSDFS 的网络安全法规，[2] FAFC 一直在与监管机构就同一网络安全风险管理失败的问题进行多方面争斗。除监管方面外，NYSDFS 的行动也构成了股东对 FAFC 及其董事会提起衍生诉讼[3]以及提出一些传闻所说的消费者集体诉讼的基础。

警告和宽限期似乎已经结束，因为美国证券交易委员会（SEC）和纽约州金融服务部（NYSDF）目前正在使用其执法权力来确保各公司实施稳健的网络安全风险管理系统。[4]随着网络攻击不断出现并持续演变，公司的网络安全风险管理工作和相关控制以及公司治理将受到监管审查只是迟早的问题。为了避免巨额罚款和其他处罚，公司需要制定全面的网络安全风险管理标准，并定期测试和对其效力进行升级。

FAFC 案

FAFC 提供住宅和商业房地产的产权保险以及交割和托管服务。2019 年 5 月 24 日，一名网络安全记者通知 FAFC 的投资者关系人员，告知 FAFC 用于共享与所有权和托管交易相关的文档图像的网络应用程序存在网络安全漏洞，该漏洞暴露了 8 亿多份房地产交易文档中的敏感个人信息，包括银行账号、抵押和税务记录、社会保险号码、电汇交易收据和驾照图像。在 FAFC 关闭对该网络应用程序的外部访问后，记者发表了一篇关于该漏洞的文章。[5]

2019 年 5 月 28 日，即文章发布后的第一个交易日，FAFC 向 SEC 提交了一份 8-K 表格和有关漏洞的新闻稿。负责 8-K 表格披露的高级管理人员不知到 FAFC 信息安全人员几个月前就了解到了这一漏洞，但未能解决问题，最重要的是就 SEC 执法行动一事，在记者发出警告之前未能将该问题告知高级信息安全管理层。此外，在记者的警告和 8-K 表格披露之间，FAFC 首席信息安全官和首席信息官了解到信息安全人员事先知道该漏洞，但未能将这一事实告知负责 8-K 表格披露的 FAFC 高级管理人员（包括首席执行官和首席财务官）。

SEC 执法行动：未知的网络安全风险是执法的基础

2021 年 6 月 15 日，美国证券交易委员会（SEC）宣布它已经通过 FAFC 同意停止命令以及 487,616 美元的民事罚款与 FAFC 就其执法行动达成了和解。SEC 发现，FAFC 与网络安全风险相关的披露控制和程序存在缺陷，违反了经修订的 1934 年《证券交易法》第 13a-15（a）条规定，而该条款要求根据《证券交易法》第 12 条注册的发行人保有披露控制和程序，以确保按照 SEC 规则和表格的要求及时准确地报告信息。

SEC 得出结论认为，FAFC 高级管理人员在批准 8-K 表格时，缺乏必要的信息来评估 FAFC 的网络安全响应能力和网络应用程序漏洞的风险程度。尽管从事提供与房地产交易相关的服务，SEC 确定 FAFC"...没有任何与网络安全相关（包括涉及可能泄露数据的事件）的披露控制和程序。"[6] 在宣布此次和解时， SEC 执法部门的网络单位负责人警告说："发行人必须确保对投资人重要的信息向负责披露的人报告。"[7]

SEC 针对 FAFC 的行动在多个层面上都值得注意。首先，这一执法行动是在将近十年的网络安全风险警告之后，首次以违反 13a-15（a）规则中有关披露控制和程序的行为为由做出的。在其 2011 年关于网络安全风险和网络事件披露义务的初始指南中，SEC 警告各公司应评估其网络安全事项披露控制和程序中的潜在缺陷。[8] 2018 年，SEC 对该指南进行了部分更新，并特别强调"保有与网络安全风险和事件相关的全面政策和程序的重要性"，以确保在公司层面上处理和报告有关网络安全风险和事件的相关信息，使高级管理层能够作出准确的披露和相关认证。[9] 自 2018 年指南发布以来，SEC 发布了关于制定网络安全风险治理标准的额外建议。[10] 随着 FAFC 行动，SEC 已从指南转向执行，增加了上市公司在未能实施健全的网络安全风险管理系统和相关披露程序的情况下的风险。

在另一个层面上，该行动延续了 SEC 最近的趋势，即通过与财务报告内部控制以及披露控制和程序相关的规则来处理披露相关事宜。[11] 通过避开依据证券披露法提出的索赔，如《交易法》第 10 条和第 18 条及其下的规则，SEC 不需要确定披露是否具有重大误导性，或者未能披露是否涉及做出披露的人员的科学行为或其他应受谴责的行为或知识。相反地，SEC 简化了为确定公司控制和程序是否提醒高级管理人员注意特定事实和信息的调查。

显然地，SEC 正在透过控制和程序执法行动来推动网络披露，并迫使公司治理的标准与委托说明书薪酬披露和分析章节中受到强制揭露要求影响的对高管薪酬做法相似。然而，由于网络攻击的普遍性和严重性，公司的网络安全风险管理系统落入监管（和原告律师）的准心只是早晚的问题。

NYSDFS 的行动

SEC 并不是唯一一个利用其监管权力迫使公司开发综合网络安全风险管理系统的机构。NYSDFS 是负责监管纽约金融服务业（包括银行、保险公司和抵押贷款服务机构）的州政府机构。NYSDFS 发布了详细的网络安全法规，于 2019 年 3 月全面生效，其中规定了最低限度但全面的网络安全风险管理系统要求。[12] 根据网络安全法规，纽约金融服务行业必须制定有关 14 个网络安全风险因素的书面政策 [13]、书面事件回应计划 [14]、进行年度渗透测试 [15]、提交年度证书 [16] 及其他更多措施。

2020 年 7 月 22 日，纽约市 NYSDFS 宣布对 FAFC 的网络安全指控。这些指控将于今年晚些时候举行听证会，每次违规将被处以高达 1000 美元的罚款，8 亿份文件中的每一次非公开信息的泄露都构成单独的违规行为。[17] 对 FAFC 的指控是 NYSDFS 首次的网络安全执法行动；然而，在一年内，NYSDFS 宣布了三个有关违反网络安全条例的和解，罚款从 150 万美元到 300 万美元不等。[18]

关键要点

为避免重大监管和民事索赔、罚款和处罚，上市公司应仔细审查其网络安全风险管理系统、以及其有关网络安全风险的财务报告和披露控制和程序的内部控制。这些控制、程序和网络风险管理政策应由多功能团队进行审查，包括来自信息技术、内部审计、风险管理的人员，尤其对金融服务等高度监管行业运营的公司或其他面向消费者的公司，应由具有网络专业知识的法律顾问审查。公司应考虑加强对各种网络安全风险因素的书面政策和程序，建立有效的报告结构，将网络安全漏洞和网络事件传达给高级管理人员，制定监测和测试协议，编写书面事件回应计划；评估各种技术漏洞。此外，由于网络攻击和网络安全风险的性质不断演变，应考虑定期审查和测试网络安全治理标准。此外，在了解到网络安全漏洞和/或网络事件后，上市公司需要快速评估其对投资者、SEC 和其他监管机构的报告义务。

有关如何避免 SEC 针对网络安全风险采取执法行动的更多信息或指导，请联系 Holland & Knight 的上市公司和证券团队或数据策略、安全和隐私团队的作者或其他成员。

附注

[1] 参见美国证券交易委员会 2021 年 6 月 15 日的新闻稿：美国证券交易委员会指控发行人网络安全披露控制失败和相关的美国证券交易委员会指令。

[2] 参见 NYSDFS 于 2020 年 7 月 22 日发布的新闻稿：金融服务部宣布对一家贷款所有权保险提供商收取网络安全费用，因为该提供商披露了数百万份包含消费者个人信息的文件以及相关费用。

[3] *Hollet v. Gilmore*，案件编号 1:20-cv-01620（D. Del. 2020 年 11 月 25 日）；另见"美国首位因数据泄露而被提起衍生诉讼的人"，Rachel O'Brian，法律 360，2020 年 11 月 30 日。

[4] 事实上，在 Holland & Knight 提示文章发布的同时，许多上市公司正在接受 SEC 关于 SolarWinds 网络攻击的影响的调查，并表示 SEC 打算对未能适当披露攻击影响的行为做出行动。

[5] 见"第一美国金融公司泄露了数亿份产权保险记录"，Brian Krebs，Krebs On Security，2019 年 5 月 24 日。

[6] SEC 命令。

[7] SEC 于 2021 年 6 月 15 日发布的新闻稿：SEC 指控发行人网络安全披露控制失败。

[8] 见美 SEC 公司金融部，CF 披露指南：主题 2，2011 年 10 月 13 日。

[9] 9 见 SEC《关于上市公司网络安全披露的委员会声明和指南》，2018 年 2 月 21 日。

[10] 参见，例如，网络安全和弹性观察，SEC 合规和检查办公室。

[11] 参见，例如，美国 SEC 的停止令和针对 Andeavor LLC 的 2000 万美元民事罚款，因其未能维持与订立 10b5-1 股份回购计划相关的充分内部控制。

[12] 见《纽约法规、规则和条例》（CRR-NY）第 23 章第 500 部分。

[13] 23 CRR-NY§500.3。

[14] 23 CRR-NY§500.16。

[15] 23 CRR-NY§500.5

[16] 23 CRR-NY§500.17

[17] 参见 NYSDFS 于 2020 年 7 月 22 日发布的新闻稿：金融服务部宣布对一家贷款所有权保险提供商提出网络安全方面的指控，因为该提供商泄露了含有消费者个人信息的数百万份文件。

[18] 参见 NYSDFS 2021 年 3 月 3 日发布的新闻稿，NYSDFS 宣布与抵押贷款贷款人进行网络安全和解；NYSDFS 新闻稿，日期为 2021 年 4 月 14 日，DFS 总监 Lacewell 宣布与被许可的保险公司达成网络安全和解；NYSDFS 新闻稿日期为 2021 年 5 月 13 日，DFS 总监 Lacewell 宣布与...人寿保险公司达成网络安全和解。

Tax and Non-Tax Considerations when Drafting Irrevocable Trusts

By Kenny N. Jefferson

An irrevocable trust is an incredibly flexible planning tool. But with great flexibility comes the need to make many decisions. This article provides a guide for helping clients identify and work through some fundamental decisions so the final product will reflect their non-tax and tax objectives. The advice is limited to standard irrevocable trusts. Other considerations are raised by charitable trusts, grantor retained annuity trusts, irrevocable life insurance trusts, and other special purpose trusts.

NON-TAX OBJECTIVES

A candid conversation with a client at the outset of the representation about the specifics of the beneficiaries' life circumstances is a necessary first step in structuring a trust agreement that furthers the client's objectives.

Financial security. A common non-tax objective is providing security to the client's family and other loved ones. But many also wish to limit the extent to which young adults have direct access to the resources set aside for them until it is clear that they have the maturity and good judgment to use the resources responsibly.

Spendthrift planning. Often another non-tax objective is protecting beneficiaries, especially those with substance abuse or other mental health challenges, from the poor decisions they likely would make if given control over the assets.

Creditor protection. Most clients are interested in protecting trust assets from the claims of the beneficiaries' creditors, including divorcing spouses.

Trust structure. Once a client's non-tax objectives are clear, the estate planning attorney has many tools that may prove useful. In a conventional trust, the trustee holds legal title to the trust assets in a fiduciary capacity and is charged with properly making distributions, investing the trust's assets, transacting on behalf of the trust, filing tax returns, and generally acting as a custodian to maintain the books and records of the trust. Now, however, jurisdictions are increasingly permitting the responsibilities of a trustee to be split to allow certain decision-making authority to be delegated among advisors separate from the trustee. Before taking certain actions the trustee must solicit or obtain the advisor's direction or consent.

For example, a separate advisor or group of advisors may be delegated the power to make distribution decisions concerning the trust, often called a distribution advisor, whereas another advisor may control the investment decisions (i.e., an investment advisor), sometimes in a manner unrestricted by the prudent investor rules. This structure is generally referred to as a directed trust. The division of trustee decision-making powers among advisors can help guard against a corporate trustee, in the business of mechanically administering thousands of trusts and sometimes apt to lose sight of a grantor's original intent, from exerting too much control and impeding the intended function and administration of the trust for a grantor's beneficiaries.

An additional consideration is that each state jurisdiction has its own specific laws regarding the taxation of trusts. Each jurisdiction also has differing criteria for establishing minimum contacts to serve as the basis for trust income taxation. For example, some states look to the grantor, whether living or dead, and the facts and circumstances surrounding the creation of the trust. But other jurisdictions emphasize the predominant place

of administration of the trust and focus on the trustee. Still other jurisdictions focus on the locations of primary beneficiaries receiving current distributions to establish minimum contacts for taxation of trust income. This can lead to a situation where a trust is subject to income tax in several states. Moreover, each jurisdiction also has its own laws governing trusts covering everything from permissible trustee duties and powers, to nuts-and-bolts trust administration and how, if at all, a trust may be manipulated or modified, either with or without court participation.

Distribution provisions. Distributions from the trust fund may be structured to be either mandatory or discretionary, of income only or of principal and income, under any number of broad or limited conditions, to a single beneficiary or a class of beneficiaries, and with or without restrictions to conserve the trust fund for remainder beneficiaries. A distribution structure may provide for the accumulation of the trust fund while children are still maturing and still allow discretionary distributions under limited circumstances for emergencies. Then upon the occurrence of a certain event or the attainment of a certain age by one or all of the children, the pot may split into separate trusts for the benefit of each child and commence either compulsory or discretionary distributions of income or principal.

TAX OBJECTIVES

Regardless of whether a client seeks assistance with tax objectives in mind, the estate planning attorney assisting him must identify the alternatives and decisions that go along with them.

Grantor vs. non-grantor. One fundamental tax-focused decision when structuring a trust is whether the trust should be a grantor trust or a non-grantor trust. If the former, the grantor will be responsible for paying the income tax on income (including capital gains) produced by the trust assets. If the latter, the trust will pay its own taxes. A grantor trust effectively allows the grantor to make additional gifts to the trust beneficiaries without using additional gift tax exemption or paying gift tax.

Generation-skipping transfer tax. Another tax-focused decision is whether to structure the trust to be fully exempt from the generation-skipping transfer (GST) tax. This is an important consideration for clients that are intending to benefit "skip-persons," or someone 37½ years younger than the donor, generally grandchildren and more remote descendants. So, a grantor wanting to create a trust to benefit her grandchildren and more remote descendants would want to consider all of the following: (i) whether during the grantor's life to make the trust a grantor or non-grantor trust, (ii) application of unused GST exemption to the transfer of assets to fund the trust, and (iii) depending on the ages of the grandchildren, whether an accumulation period would be useful before the beneficiaries become eligible for, or entitled to, distributions.

CONCLUSION

Although not exhaustive, the above considerations will assist you when undertaking irrevocable trust planning with clients.

Reprinted with permission from the American Bar Association's Probate & Property Magazine

草拟不可撤销信托时的税务和非税务考量

原文作者：**Kenny N. Jefferson**

不可撤销信托是一种极其灵活的规划工具。但伴随着巨大的灵活性而来的是需要做出许多决定。本文章提供了一个指南，帮助客户确定并完成一些重大决定，以便最终产品能够反映其非税务和税务目的。本建议仅限于一般的不可撤销信托。慈善信托、授予人保留年金信托、不可撤销人寿保险信托和其他特殊目的信托有其他考量因素。

非税务目的

在开始代表时，与客户就受益人生活情况的细节进行坦诚对话，是规划促进客户目的的信托协议必要的第一个步骤。

财务安全。一个通常的非税务目的是为客户的家人和其他亲人提供安全保障。但许多人也希望限制年轻人直接获得为他们预留的资源的程度，直到确定他们成熟了并具有良好的判断力来负责任地使用资源。

节俭的计划。另一个经常的非税收目的是保护受益人，尤其是保护那些有药物滥用或其他精神健康问题的受益人，使他们免受如果让他们控制资产时可能做出的糟糕决定的情况。

债权人保护。大多数客户均有意保护信托资产免受受益人的债权人（包括离婚配偶）的索赔。

信托结构。一旦客户的非税务目的明确，财产规划律师就拥有许多可能证明有用的工具。在传统信托中，受托人以受托人身份持有信托资产的法律所有权，并负责妥善分配、投资信托资产、代表信托进行交易、提交纳税申报表、以及通常作为保管人维护信托账簿和记录。然而，现在，越来越多司法管辖区越来越多允许将受托人的责任划分，以允许将某些决策权委托给与受托人不同的顾问。在采取某些行动之前，受托人必须征求或获得顾问的指示或同意。

例如，**一名**单独的顾问或一组顾问可能被授权做出有关信托的分配决策，通常称为分配顾问，而另一名顾问可能控制投资决策（即投资顾问），有时以不受审慎投资者规则限制的方式进行投资。这种结构通常被称为定向信托。顾问之间的受托人决策权划分有助于防止因公司受托人机械性地管理数千个信托而有时容易忽视授予人的原始意图，从而避免对授予人的受益人施加过多的控制及妨碍信托的预期功能和管理。

另一个考量因素是，每个州的司法管辖区都有自己关于信托征税的具体法律。每个司法管辖区也有不同的标准来建立最低限度的联系，以作为课征信托所得税的基础。例如有些州着眼于授予人，不论其在世或已过世、以及围绕设立信托的事实和情况。但其他司法管辖区强调信托管理的主导地位，并将重点放在受托人身上。还有一些司法管辖区将重点放在接受当前分配的主要受益人的所在地，以建立信托收入征税的最低联系。这可能导致信托必须在在几个州缴纳所得税的情况。此外，每个司法管辖区都有自己的法律管辖信托，涵盖从允许的受托人职责和权力到具体的信托管理细节、以及在有或没有法院参与的情况下如何操纵或修改信托。

分配规定。信托基金的分配可以是强制性的，也可以是自由裁量的，可以只分配收入，也可以分派本金和收入，可以受制于在任何数量的广泛或有限的条件、可以分配给单一受益人或某一类别的受益人，并且可以具有或不具有为其余受益人保留信托基金的限制。分配结构可规定在儿童尚在成长时积累信托基金，并允许在有限的

紧急情况下酌情分配。然后，当某一事件发生或一名或所有子女达到某一年龄时，资金可为每个子女的利益分成单独的信托，并开始强制性或任意分配收入或本金。

税收目的

无论客户是否寻求税务目的方面的帮助，协助他的财产规划律师必须确定与之相关的备选方案和决策。

授予人与非授予人。在规划信托时，一个重大的以税收为重点的决策是该信托是授予人信托还是非授予人信托。如果是前者，授予人将负责支付信托资产产生的收入（包括资本收益）的所得税。如果是后者，信托将自行纳税。授予人信托有效地允许授予人向信托受益人提供额外的赠与，而无需使用额外的赠与税豁免额度或支付赠与税。

代际转移税。另一个以税收为重点的决策是，是否将信托结构设置为完全免除跨代转让（GST）税。对于打算作成对"跨代人士"或比自己年轻 37½岁的人（通常是孙辈和更远的后代）有益安排的客户，这是一个重要的考虑因素。因此，一个希望建立一个信托，以使她的子孙和更久远后代的受益的人将要考虑以下所有事项：（i）是否在授予人在世期间，将信托作成为授予人信托或非授权人信托；（ii）对资产的移转适用尚未使用的 GST 豁免已作为对信托基金注入；以及（iii）根据孙辈的年龄，在受益人有资格或有权获得分配之前，设立一积累期是否有帮助。

结论

尽管并非详尽无遗，但上述考量因素将有助于您与客户进行不可撤销的信托的计划。

本复制获得美国律师协会遗产认证及财产杂志的同意。

GSA Mandates Disclosure of Foreign Ownership/Financing of High-Security Leased Spaces

New Rule Applies to Buildings Leased to the U.S. Government

By Ronald A. Oleynik, Libby Bloxom and Robert C. MacKichan Jr.

HIGHLIGHTS

- The new General Services Administration (GSA) Rule imposes disclosure requirements regarding the foreign ownership of prospective lessors of "high-security leased space" (property leased to the federal government having a security level of III or higher) and mandates access limitations on such foreign-owned lessors.
- As of June 2021, GSA estimates about 16 percent of the existing leases in its portfolio (or 1,263 out of 7,860 leases) constitute "high-security leased spaces."
- Although the Rule is effective immediately, GSA is seeking public comments and will consider such comments when forming the final rule. The deadline for submitting a comment was Aug. 30, 2021.

The General Services Administration (GSA) amended the General Services Administration Acquisition Regulations (GSAR) via an interim rule (Rule) – effective June 30, 2021 – to incorporate disclosure obligations of foreign ownership of high-security spaces leased to the federal government. Specifically, the Rule adds two new requirements to the GSAR: 1) lessors must make a representation regarding foreign ownership or foreign financing of "high-security leased spaces" – spaces with Facility Security Levels III, IV or V – and 2) foreign-owned or foreign-financed leases must limit access to foreign lessors.

BACKGROUND

The Rule stems from the Secure Federal Leases from Espionage and Suspicious Entanglement Act (Act), which became law on Dec. 31, 2020, and imposed requirements on federal agencies to obtain ownership information of foreign-owned buildings for high-security leases.

The Act was passed in response to a 2017 Government Accountability Office (GAO) report, which revealed certain federal agencies were not aware that their high-security spaces were located in foreign-owned buildings. It also revealed that GAO was unable to identify the ownership information of approximately one-third of the government's high-security leases. GAO concluded that the use of such spaces for classified operations and storage of sensitive data created security risks and national security concerns of espionage and unauthorized cyber and physical access.

APPLICABILITY OF THE RULE

The Rule is applicable to new leases by GSA and the head of any federal agency that has independent statutory leasing authority; but will not apply to leases with the U.S. Department of Defense and the Intelligence Community agencies, as such agencies are already subject to similar ownership disclosure

requirements pursuant to the 2018 National Defense Authorization Act. New leases include not only lease awards but also options for current leases (e.g., renewal, succeeding and replacing leases and other novations), lease extensions and ownership changes for high-security leased spaces entered into on or after June 30, 2021. Thus, while the Rule is effective immediately, there are no retroactive disclosure obligations.

INFORMATION REQUIRED TO BE DISCLOSED

The Rule mandates that lessors disclose, through a newly imposed representation at 48 C.F.R. § 552.270-33, whether the immediate owner or the highest-level owner of the building, as well as any entity involved in the financing, is a foreign person or entity and the associated country of citizenship or organization. "Immediate owner" is defined as "an entity that has direct control of the . . . lessor," and "highest-level owner" is defined as "the entity that owns or controls [the] immediate owner . . ." The following factors may indicate control: "ownership or interlocking management, identity of interests among family members, shared facilities and equipment, and the common use of employees."

The representation also requires the lessor to state whether the lease is financed by a foreign entity, and if so, lessors must disclose the legal name, unique entity identifier, physical address and country of foreign financing. "Financing" captures debt and equity fundraising for the lease, including acquisition, maintenance and construction of and improvements to the property.

In addition to foreign ownership disclosure requirements, applicable leases will be required to include a new GSAR clause at 48 C.F.R. § 552.270-34, which provides access restrictions for the foreign owner and property manager. Specifically, lessors and property managers will be required to obtain approval from the government before accessing the leased space.

IMPACT OF THE RULE AND OTHER CONSIDERATIONS

In the event of foreign ownership or foreign financing, prior to awarding the lease, GSA or the contracting officer will coordinate and consult with the federal tenant on any security concerns and necessary mitigation measures. Once a lease is executed, the lessor will be required to verify its ownership and financing information on an annual basis.

While the Rule does not disqualify foreign-owned or foreign-financed buildings from leasing to federal agencies, it will result in enhanced scrutiny by GSA of new leases or lease novations. Importantly, these new requirements are separate from the jurisdiction of the Committee on Foreign Investment in the United States (CFIUS) in connection with reviews of covered real estate transactions (see a 2019 Holland & Knight-authored article related to CFIUS's jurisdiction of "covered real estate transactions"). Given the interagency dialogue among federal government agencies, the Rule also may increase CFIUS's reviews of covered real estate transactions.

Although the Rule is effective immediately, GSA is seeking public comments and will consider such comments when forming the final rule. The deadline for submitting a comment was Aug. 30, 2021.

For more information on the implications of these newly imposed requirements or for assistance on complying with such requirements, please contact the authors or another member of Holland & Knight's International Trade Group or GSA Leasing & Federal Real Estate Team.

美国总务管理局要求对高度安全等级租赁空间的外国所有权/融资进行披露

适用于租赁给美国政府的建筑物的新规定

原文作者：**Ronald A. Oleynik、Libby Bloxom 及 Robert C. MacKichan Jr.**

重点摘要

- 新的美国总务管理局（GSA）的规则对"高度安全等级租赁空间"（租赁给联邦政府的安全等级为 III 或更高的财产）的预计出租人的外国所有权加诸了披露的要求，并规定对此类外国所有权的出租人的访问限制。
- 截至 2021 年 6 月，GSA 估计其租赁列表中约 16%的现有租赁（或 7,860 个租赁中的 1,263 个）被视为"高度安全等级租赁空间"。
- 尽管规则立即生效，但 GSA 正在寻求公众意见，并将在制定最终规则时考虑此类意见。提交意见的截止日期是 2021 年 8 月 30 日。

美国总务管理局（GSA）通过一项临时规则（规则）修订了《美国总务管理局收购条例》（GSAR）——自 2021 年 6 月 30 日起生效——以纳入租赁给联邦政府的高度安全等级空间的外国所有权的披露义务。具体而言，该规则在 GSAR 中增加了两项新的要求：1）出租人必须就"高度安全等级租赁空间"（设施安全等级为 III、IV 或 V 的空间）的外国所有权或外国融资作出陈述；及 2）外国所有权或外国融资租赁物必须限制外国出租人的进入。

背景

该规则源于《联邦租赁物情报活动和可疑牵连防制法案》（法案），该法案于 2020 年 12 月 31 日成为法律，并要求联邦机构获取关于高度安全等级租赁用外资建筑物的所有权信息。

该法案是针对 2017 年政府问责局（GAO）的报告而通过的，该报告显示，某些联邦机构不知道其高度安全等级空间位于外资的建筑内。报告还显示，GAO 无法识别大约三分之一的政府高度安全等级租赁的所有权信息。GAO 的结论是，将此类空间用于机密操作和敏感数据的存储会产生安全风险和国家安全问题，包括情报活动和未经授权的网络和实体进入。

规则的适用

该规则适用于 GSA 和任何拥有独立法定租赁权的联邦机构负责人的新租赁；但不适用于与美国国防部和情报机构的租赁，因为根据 2018 年《国防授权法》，这些机构已经受到类似所有权披露要求的约束。新租约不仅包括租约授予，还包括当前租约的选择权（例如续约、继受和替换租约以及其他更替）、2021 年 6 月 30 日或之后签订的高度安全等级租赁空间的租约延期和所有权变更。因此，尽管该规则立即生效，没有追溯披露的义务。

需要披露的信息

该规则要求出租人通过 48 C.F.R.§552.270-33 中新规定的陈述，披露建筑物的直接所有人或最上层所有人以及参与融资的任何实体是否为外国人或实体以及相关国籍或组织。"直接所有人"被定义为"对……出租有直接控制权的实体，而"最上层所有人"被定义为"拥有或控制直接所有者的实体……"以下因素可能显示出控制："所有权或交互管理、家庭成员的利益的一致性、共享设施和设备以及员工的共同使用。"

该陈述还要求出租人说明租赁是否由外国实体融资，且如是的话，出租人必须披露外国融资的法定名称、特定实体辨识身份、实际地址和国家。"融资"包括租赁的债务和股权融资，包括物业的收购、维护、建设和改善。

除外国所有权披露要求外，适用规则的租约还需要包括 48 C.F.R.§552.270-34 中的新 GSAR 条款，该条款为外国所有人和财产管理人加上访问限制。具体而言，出租人和物业管理人在进入租赁场地前必须获得政府的批准。

规则的影响和其他考虑因素

如果存在外国所有权或外国融资，在授予租赁之前，GSA 或合同官员将与联邦承租人就任何安全问题和必要的缓解措施进行协调和协商。一旦签订租约，出租人将被要求每年核实其所有权和融资信息。

虽然该规则并没有取消外国拥有或外国融资的建筑物出租给联邦机构的资格，但它将导致 GSA 加强对新租赁或租赁更新的审查。重要的是，这些新要求独立于美国外国投资委员会（CFIUS）对相关房地产交易的审查管辖权（参见关于 CFIUS 对"相关房地产交易"的管辖权，2019 年 Holland & Knight 撰写的一篇文章）。考虑到联邦政府机构之间的机构间对话，该规则还可能增加 CFIUS 对所涵盖房地产交易的审查。

虽然规则立即生效，但 GSA 正在寻求公众意见，并将在制定最终规则时考虑该等意见。提交意见的截止日期是 2021 年 8 月 30 日。

有关这些新规定的影响或如何遵守这些要求的协助的更多信息，请联系作者或 Holland & Knight 国际贸易团队或 GSA Leasing & Federal Real Estate 团队的其他成员。

About This Newsletter
有关本期刊

Information contained in this newsletter is for the general education and knowledge of our readers. It is not designed to be, and should not be used as, the sole source of information when analyzing and resolving a legal problem. Moreover, the laws of each jurisdiction are different and are constantly changing. If you have specific questions regarding a particular fact situation, we urge you to consult competent legal counsel. Holland & Knight lawyers are available to make presentations on a wide variety of China-related issues.

本期刊所刊载的信息仅供我们的读者为一般教育及学习目的使用。本期刊并不是为作为解决某一法律问题的唯一信息来源的目的所设计，也不应被如此使用。此外，每一法律管辖区域的法律各有不同且随时在改变。如您有关于某一特别事实情况的具体法律问题，我们建议您向合适的律师咨询。美国霍兰德奈特律师事务所的律师能够对许多与中国相关的问题提出他们的看法及建议。

About the Authors
关于本期作者

Libby Bloxom focuses her practice on a broad range of international trade regulatory and transactional matters, including foreign direct investment, industrial security, export control, sanctions and customs matters. Her practice also involves assisting clients in corporate jet transactions and structuring of corporate aircraft operations to comply with Federal Aviation Administration (FAA) regulations. She also has experience handling commercial transactions in areas such as procurement and disposition, distribution, technology and intellectual property transfer, licensing and outsourcing of business processes and professional services primarily in the aviation, supply chain management and transportation industries.

Daniel J. Barsky regularly represents clients in intellectual property (IP), information technology (IT) and data-related licensing and transactional matters, including mergers and acquisitions (M&A), private equity transactions, joint ventures, and multilateral and multinational licensing agreements. His clients call upon him to navigate complex transactions involving IP, IT and data assets. He assists and advises clients with navigating the complexities of transactions involving intangible assets such as patents, trademarks, copyrights, trade secrets and data, brand licensing and distribution agreements, blockchain technology such as cryptocurrency and non-fungible tokens (NFTs), software and technology licensing agreements, and transition services agreements.

Shardul Desai is a cybersecurity, data privacy, and white collar defense and government investigations attorney. He has extensive experience in handling cyber intrusions and data breaches, trade secret thefts, emerging technology matters and complex white collar investigations. With a computer science and physics background, he is highly skilled and knowledgeable to advise companies on novel issues at the intersection of law, technology and data privacy. He is also a Certified Information Privacy Professional in the United States (CIPP/US) with the International Association of Privacy Professionals (IAPP). He previously was a federal prosecutor in the Cyber and National Security Section and the Economic Crimes Section at the U.S. Attorney's Office for the Western District of Pennsylvania.

Kenny N. Jefferson is a private wealth services attorney who focuses his practice on advising high-net-worth individuals and families on complex estate, gift and generation-skipping transfer (GST) tax planning issues, managing tax compliance challenges and achieving non-tax goals. He has experience drafting core estate planning documents, including wills, all manner of trusts, financial powers of attorney (POA) and healthcare directives. He advises and helps implement trust modification techniques, probate matters and high-net-worth estate administration, business planning and entity formation.

Robert C. MacKichan Jr. has a multifaceted practice that involves decades of experience in litigation, government contracts, real estate and public policy issues associated with federal government real estate. Clients call on him for his substantive knowledge and extensive relationships in Washington, D.C., and throughout the nation to handle myriad government real estate-related matters. Those include: all aspects of the competitive federal government lease procurement process; lease administration issues arising under the terms of federal leases; filing or defending formal challenges (bid protests) to the competitive lease procurement process; representation of owner/lessors to pursue claims against the federal government, or defending owner/lessors in claims filed by the government, pursuant to the Contract Disputes Act; government holdovers in leased space after expiration of federal leases and federal condemnation of a leasehold interest; disposal of government real estate; federal statutory and regulatory issues associated with the assignment of a lease pursuant to a sale or purchase of a property with federal tenants; and the statutory and regulatory requirements for assignment of rents in the financing of a federal lease

Ronald A. Oleynik is head of the International Trade Practice, and focuses his practice in the area of international trade regulation. His experience includes a broad range of industrial security, customs, export control, trade policy, and public and private and international trade matters. He has substantial experience in assisting clients in complying with U.S. trade embargoes and economic sanctions programs involving countries such as Cuba, Iran, North Korea, Russia and Syria. He works frequently with the Treasury Department's Office of Foreign Assets Control, which is responsible for implementing, administering and enforcing sanctions regulations that restrict business transactions involving designated countries and their nationals.

Ira N. Rosner has more than three decades of experience helping entrepreneurs and corporate management teams create, fund, manage, grow and capitalize on their businesses. He has worked with a wide variety of companies, ranging from startup ventures to Fortune 100 enterprises, in a wide array of industries, including construction, healthcare, real estate (including REITs), pharmaceuticals, aerospace and aviation, agriculture, energy, manufacturing, high tech, life sciences, retail, business outsourcing, telecommunications and insurance. In addition, he is highly experienced in both public and private equity and debt securities offerings, as well as the sale and acquisition of public and privately held companies.

Contact Our China Practice Attorneys | 与我们的 China Practice 律师联系

Primary Contacts 主要联系人：

Hongjun Zhang, Ph.D. 张红军博士
Washington, D.C.
+1.202.457.5906
hongjun.zhang@hklaw.com

Mike Chiang 蒋尚仁律师
San Francisco
+1.415.743.6968
mike.chiang@hklaw.com

Juan M. Alcala | Austin
+1.512.954.6515
juan.alcala@hklaw.com

Leonard A. Bernstein | Philadelphia
+1.215.252.9521
leonard.bernstein@hklaw.com

Christopher W. Boyett | Miami
+1.305.789.7790
christopher.boyett.@hklaw.com

Vito A. Costanzo | Los Angeles
+1.213.896.2409
vito.costanzo@hklaw.com

Josias N. Dewey | Miami
+1.305.789.7746
joe.dewey@hklaw.com

R. David Donoghue | Chicago
+1.312.578.6553
david.donoghue@hklaw.com

Jonathan M. Epstein | Washington, D.C.
+1.202.828.1870
jonathan.epstein@hklaw.com

Leonard H. Gilbert | Tampa
+1.813.227.6481
leonard.gilbert@hklaw.com

Enrique Gomez-Pinzon | Bogotá
+57.1.745.5800
enrique.gomezpinzon@hklaw.com

Paul J. Jaskot | Philadelphia
+1.215.252.9539
paul.jaskot@hklaw.com

Adolfo Jimenez | Miami
+1.305.789.7720
adolfo.jimenez@hklaw.com

Roth Kehoe | Atlanta
+1.404.817.8519
roth.kehoe@hklaw.com

Robert J. Labate | San Francisco
+1.415.743.6991
robert.labate@hklaw.com

Alejandro Landa Thierry | Mexico City
+52.55.3602.8002
alejandro.landa@hklaw.com

Jeffrey W. Mittleman | Boston
+1.617.854.1411
jeffrey.mittleman@hklaw.com

Anita M. Mosner | Washington, D.C.
+1.202.419.2604
anita.mosner@hklaw.com

Ronald A. Oleynik | Washington, D.C.
+1.202.457.7183
ron.oleynik@hklaw.com

Douglas A. Praw | Los Angeles
+1.213.896.2588
doug.praw@hklaw.com

John F. Pritchard | New York
+1.212.513.3233
john.pritchard@hklaw.com

Robert Ricketts | London
+44.20.7071.9910
robert.ricketts@hklaw.com

Luis Rubio Barnetche | Mexico City
+52.55.3602.8006
luis.rubio@hklaw.com

Francisco J. Sanchez | Tampa
+1.813.227.6559
francisco.sanchez@hklaw.com

Evan S. Seideman | Stamford
+1.203.905.4518
evan.seideman@hklaw.com

Jeffrey R. Seul | Boston
+1.617.305.2121
jeff.seul@hklaw.com

Vivian Thoreen | Los Angeles
+1.213.896.2482
vivian.thoreen@hklaw.com

Shawn M. Turner | Denver
+1.303.974.6645
shawn.turner@hklaw.com

Matthew P. Vafidis | San Francisco
+1.415.743.6950
matthew.vafidis@hklaw.com

Stacey H. Wang | Los Angeles
+1.213.896.2480
stacey.wang@hklaw.com

Charles A. Weiss | New York
+1.212.513.3551
charles.weiss@hklaw.com

Jose V. Zapata | Bogotá
+57.1.745.5940
jose.zapata@hklaw.com

Office Locations 办公室地点

Algiers | Atlanta | Austin | Bogotá | Boston | Charlotte | Chicago | Dallas | Denver | Fort Lauderdale | Fort Worth | Houston
Jacksonville | London | Los Angeles | Mexico City | Miami | Monterrey | New York | Orange County | Orlando | Philadelphia
Portland | San Francisco | Stamford | Tallahassee | Tampa | Tysons | Washington, D.C. | West Palm Beach