THOMSON REUTERS
PRACTICAL LAW™

Non-Fungible Tokens (NFTs): Overview

by BakerHostetler LLP and Practical Law Finance*

Status: **Maintained** | Jurisdiction: **United States**

This document is published by Practical Law and can be found at: **content.next.westlaw.com/w-034-6437**
Request a free trial and demonstration at: **tr.com/practicallaw-home**

A Practice Note designed to help practitioners understand non-fungible tokens (NFTs), providing an explanation of how and where NFTs are relevant to a number of major areas of legal practice. This Note also includes compliance suggestions for NFT market participants, as well as an examination of novel legal issues and compliance considerations presented by NFTs.

Non-fungible tokens (NFTs) have become the subject of much attention within the legal community because of the novel legal issues they raise and the wide range of legal practice areas that they touch on. This Note is designed to help practitioners understand NFTs, so that they can provide better advice regarding whether and how to engage with the NFT ecosystem, and also provides an explanation of how NFTs are relevant to each practice area.

Like other cryptographic assets, such as bitcoin, ether, Ethereum ERC-20 tokens, and other cryptocurrency tokens, an NFT is digital code that contains certain information and that is created, stored, and transferred on a blockchain network. NFTs that exist on the Ethereum Network are typically called ERC-721 tokens which are native to the Ethereum protocol. Like all other cryptographic assets, NFTs cannot be copied or counterfeited and exist only in one specific place at any point in time on a blockchain and in one specific cryptocurrency wallet.

The first NFT was minted in May 2014 by Kevin McCoy. NFTs were initially referred to as monetized graphics because they were created to enable artists to exercise control over their work and more strongly protect against others appropriating it without permission. Not much later, in October 2015, the first NFT project, Etheria, launched, only months after the Ethereum blockchain mainnet went live. However, it was not until 2017, when the ERC721 standard was proposed via the Ethereum Github, that the term "non-fungible token" or "NFT" was coined. NFTs started to gain marketplace recognition after the launch of CryptoPunks (see NFTs in the Art World) and other NFT projects that emerged in the summer of 2017.

All of this development set the stage for the NFT explosion that occurred in 2021 (see NFTs in the Art World).

NFT Mechanics

Who Owns an NFT?

Like ether transactions, the creation and transfer of ownership of an NFT is recorded on the blockchain to which it belongs. If Party A buys an NFT from Party B on a specified date and that NFT was created on and exists on the Ethereum blockchain, a record of the transfer of that ERC-721 token exists indelibly, in perpetuity, on the Ethereum blockchain. If an NFT is created on a different blockchain, for example, the Solana blockchain, and Party A buys an NFT from Party B on a specified date, a record of that transfer exists indelibly, in perpetuity, on that blockchain, in this case the Solana blockchain. This means that at any time, the owner of an NFT can point to the relevant blockchain and authenticate, with a high level of assurance and without the need for a third-party intermediary, ownership of that NFT.

NFTs Are Nonfungible

Nonfungibility may best be understood by first looking at its antonym: fungibility. A dollar, for example, is fungible because one dollar is functionally the same as another dollar. If Party A borrows $5 from Party B, Party A can repay Party B with any $5. It need not be the same exact $5 Party B originally lent Party A. This is because dollars are fungible. In the same way, cryptocurrencies are fungible. If Party A borrows five ether from Party B, Party A can repay Party B with any

five ether. This is because ether (like cryptocurrency in general) is fungible.

Each NFT, however, is uniquely distinct from every other NFT by virtue of a unique identification code and associated metadata that is embedded into the NFT in the moment that the NFT is created on its underlying blockchain. This is similar to any other type of unique identification number (UIN), such as a bar code on the back of an event ticket or grocery store item.

However, while traditional UINs can be altered by the third party that hosts the UIN database, the unique identification code and metadata of an NFT cannot be altered because it is recorded on the underlying blockchain. The unique identification code and associated metadata that is embedded into an NFT at creation is immutable, and verifiable, in the same way that the transactional history and record of ownership of blockchain tokens are immutable and publicly available for anyone to view and verify.

NFTs are also, by operation of their technical code, non-divisible. Whereas cryptocurrencies can be subdivided into decimal fractions, NFTs, by contrast, exist on the underlying blockchain as whole numbers only.

An NFT Links to a Media File

The NFT characteristics described above may ultimately enable enhanced recordkeeping in the physical world, such as in product supply chains or property title registries. NFT technology has also already begun to enable asset tokenization, providing the ability to represent ownership of a physical asset and to transfer title to and ownership of that asset on the blockchain without the need for third-party verification or intermediation.

However, an NFT can also be a digital collectible, meaning something with no physical existence or intrinsic value, but with a value based on popularity. NFTs have become known for their ability to record ownership of digital media. This ownership is accomplished by programming NFTs with code that provides a link to an underlying digital image, song, video, tweet, or other media that exists in digital form. This referenced asset is called the "NFT media" – typically, an image, video, or .gif.

The NFT is separate from the NFT media. While the NFT exists on its underlying blockchain, the NFT media exists in a separate digital database – often a traditional centralized or cloud-based database or a decentralized database like the Interplanetary File System (IPFS). By programming the digital location of the NFT media into the NFT, the NFT may be forever programmed to "point" to the location of the NFT media. In this way, the NFT serves to verify that the NFT media is the original, official, or genuine version of the media file. This programming is important in the digital world because a digital file can be copied an infinite number of times.

The value of an NFT may be derived from the NFT media and the associated artist, its rarity and authenticity, as well as the identity of the associated artist. The NFT authenticates the NFT media, in many respects, by proving that the NFT media was attached to the NFT by a specific person at a specific point in time. However, the NFT media cannot authenticate the NFT. For information on counterfeiting of NFTs, see Protecting Against Counterfeit NFTs.

An NFT can make one version of the media file (the NFT media) unique and, therefore, more valuable than other copies that are not attached to the NFT. In this sense, the NFT media is similar to a photograph that is part of a series that was signed and numbered by the photographer. While many copies of a photograph exist or can be printed, there is only one version with a particular number, accompanied by that particular photographer's signature. Like the number and signature, an NFT is a unique identifier that adds value to the NFT media. But whereas the photograph's numbering and signature physically exists on the photograph, the NFT is digital code pointing or linking to where that particular copy of the NFT media is stored.

Where Is the NFT Media?

The NFT media that is linked in the metadata of the NFT are generally stored in one of two ways:

- The NFT media may be stored with a location-addressed URL that is directed to a private, centralized server. This can be a private server, but the more common approach is to use an account at a cloud provider, such as Amazon Web Services.
- The NFT media may be stored on a decentralized storage network, such as IPFS.

Each method has its own benefits and risks, though the relative advantages and disadvantages, best practices, and pitfalls of each method are still the subject of uncertainty. Storing media centrally creates a risk that the image can be removed by the party that manages the URL or as the result of a hack. However, the ability to delete the image associated with an NFT benefits ecosystem participants because it allows for the permanent removal of any images that violate the law or otherwise become problematic.

For example, if an NFT includes in its media file someone's personal information and the NFT goes viral, the best

recourse might be to remove the NFT. If the image is centrally stored, the company hosting the file could be compelled to remove it. Conversely, media stored in a decentralized database, like IPFS, makes it much less likely that the media could or will be removed.

NFT media location minters should consider whether to store NFT media files on a centralized server or a decentralized server, such as the IPFS. While centralized servers give more control over the media files to, for example, upgrade the media file to an improved format, decentralized servers are more secure and accessible.

Location of NFT Information

Information relating to NFT transactions can be stored in three places:

- Personal devices of users.
- Databases of the service providers for NFT transactions.
- The blockchain network on which the NFT resides.

Because the media files themselves give the NFTs their value, ensuring the availability of those files through appropriate information security controls is likewise critically important (see NFTs: Data Privacy and Information Security Considerations).

The NFT Ecosystem

The NFT ecosystem includes several categories of service providers (which are not mutually exclusive), including:

- **Creators.** Creators not only create the underlying work but also program the smart contract and link media files or commission to have those steps completed (for example, an artist or a gaming company).
- **Minters**. Minters mint the first impression of a particular NFT on the blockchain.
- **Marketplaces.** Exchange platforms initially distribute and facilitate the transactions of NFTs.
- **Custodians.** These wallet providers hold NFTs on behalf of users.
- **Media file managers.** These platforms host the media files that are linked to the NFTs.

For details on data privacy and security concerns for these entities, see NFTs: Data Privacy and Information Security Considerations.

For information on anti-money laundering (AML) considerations for these entities, see NFTs: Applicable Anti-Money Laundering (AML) Rules and Considerations.

Notable NFT Initiatives

In 2021, NFTs received official recognition by Merriam-Webster, which added to its dictionary a definition of "non-fungible token," and commemorated the addition by auctioning an NFT version of the definition on a popular NFT marketplace. Also in 2021, the auction house Sotheby's auctioned an NFT of the source code for the creation of the world wide web by British computer scientist Tim Berners-Lee, reportedly selling for $5.4 million to an anonymous buyer.

NFTs in the Art World

NFTs have a relationship to digital art and can serve as an indicator that an artist has blessed a certain copy of art, similar to a signature. In many ways, digital artist Beeple's $70 million sale in early 2021 of a .JPG file consisting of a collage of his photographs taken during a period of 5,000 days heralded a new age of digital art as a major asset class. The sale reportedly was the third most expensive work sold by a living artist at auction, and was accomplished through Christie's, an auction house associated more closely with auction sales of tangible works by artists such as Picasso and Monet.

News throughout 2021 continued to affirm the emergence of NFT digital art. For example, Christie's auctioned nine rare/early NFTs called CryptoPunks, launched in 2017, which collectively sold for nearly $17 million, and Sotheby's auctioned off the NFT CryptoPunk 7523 for $11.7 million, one of 28 NFTs that the auction house sold during the course of one week, which totaled more than $17 million in sales.

The NFT marketplace has evolved and many NFT projects derive value from offering not just a collectible token but a token that functions as a membership card in a club, as a ticket of admission to exclusive content, events, and experiences, and as a means of access to loyalty card programs. For example, the popular Bored Ape Yacht Club NFT project promotes that its NFTs double as membership to a club for apes. Auctions, including auctions of two bundles of NFTs entitled 101 Bored Ape Yacht Club and 101 Bored Ape Kennel Club, designed by Yuga Labs, fetched more than $24 million at auction. By December 2021, Sotheby's was reporting that its sale of NFT works for the year accounted for $100 million in revenue.

Though the NFT market since cooled with the onset of the so-called crypto winter, a 2023 mini resurgence included an auction of NFTs held by bankrupt crypto hedge fund Three Arrows Capital, which fetched almost $13.5 million at Sotheby's auction house in May and June of 2023.

NFT Contractual Issues

Common Types of NFT Contractual Relationships

Participants in the fast-moving but legally uncertain NFT marketplace can maximize their business opportunities and mitigate risk by clearly delineating their specific roles and defining where their obligations begin and where their responsibilities end. Understanding and defining each party's role is critical. Some of the key contractual relationships that NFT market participants can expect to encounter include:

- **Seller terms of use and rights in the NFT.** The artist creating the NFT media, or the company that commissions it as a work-for-hire, legally owns the copyright in the artwork. The copyright owner, among other rights, retains the rights to reproduce and make derivative works of the NFT media. Like buying a painting, ownership of the NFT media itself does not include ownership of the rights bestowed under copyright law unless expressly granted by the copyright owner. Unless the owner conveys these rights in selling the NFT, a buyer does not automatically receive the right to commercially exploit the artwork. The terms of use for the NFT sale govern what an NFT buyer can and cannot do with the NFT and NFT media. For more information on intellectual property and NFTs, see Article, NFTs and Intellectual Property.
- **Trading platform terms of use and agreements.** Trading platforms where NFTs can be created, listed, sold, or bought have terms of use that govern the responsibilities of the NFT marketplace operator towards its customers, as well as disclaimers regarding certain liabilities the platform purports not to assume. These terms of use also apply between buyers and sellers of the NFTs featured on the trading platform. NFT trading platforms may also enter into specific agreements with NFT sellers or technical vendors.
- **Technical vendor agreements.** NFT sellers often hire technical vendors to perform NFT customizations and other deliverables on behalf of the seller, such as creating or minting NFTs, processing NFT sales, or providing cloud accounts or decentralized storage solutions for hosting NFT media. These agreements may include certain work-for-hire provisions.
- **Cryptocurrency payment processor and exchange agreements.** Cryptocurrency payment processors allow NFT sellers to accept cryptocurrency payments and convert those cryptocurrency payments into fiat currency. In some cases, these services may extend to exchange and wallet-hosting services that allow NFT sellers to store cryptocurrency, and sometimes NFTs, in hosted wallets. These agreements govern the use of cryptocurrency payment gateways and cryptocurrency and NFT custody for NFT sellers.
- **Sale agreements related to commercial exploitation of NFTs.** Third-party vendors may provide display and viewing opportunities for NFT owners, such as digital art frames that give NFTs a lifelike form and virtual "land" (for example, digital "malls") to display NFTs. Opportunities for use of NFTs in the metaverse may also be offered by certain third-party vendors. Terms of use, and sometimes bespoke agreements, govern relationships with these vendors.

Key Issues to Consider in NFT Contract Negotiation

When negotiating NFT-related agreements:

- On the seller side, the main goal is often to secure future revenue from an NFT through initial sales and perpetual royalties.
- On the buyer side, the main goal is often to leverage the NFT for various consumptive or other benefits.
- From the perspective of a third-party vendor, the main goal is to extract the value of the deal without lingering obligations after performance is completed.

These different interests mean an increased focus on negotiation over rights, such as:

- The underlying intellectual property rights of the seller in the NFT.
- Resale limitations of the buyer.
- Controlled access by the third-party vendor.

As these negotiations develop, interested parties need to consider certain key contractual provisions, including the following.

Defining Services Provided

Vendors should clearly define the scope of their services and avoid tertiary obligations that extend past those delineated under their use or service agreements. Terms and conditions for the sale of an NFT in the primary marketplace should align with consumer protection laws to prevent misleading a buyer into buying stolen work, a trademarked brand, or a celebrity likeness.

Arranging Perpetual Royalties

It is in the artist's and the NFT seller's best commercial interest to receive future royalties from subsequent

sales of the NFT in the secondary marketplace. After all, royalties can grow over time as the NFT appreciates in value in the secondary market. To the greatest extent practicable, royalty rights should be both articulated in contract terms and programmed into smart contract code, to ensure that NFT artists and sellers receive royalties as agreed.

Specifying Rights in the NFT Media

The right to exploit the NFT for commercial gain or just commercial purposes generally depends in large part on whether, and to what extent, the seller actually conveys the underlying intellectual property rights with the transfer of the NFT. The rights of NFT sellers and buyers should be explicitly defined in this regard. Key intellectual property issues to consider include rights:

- In the media used to generate the NFT media.
- Retained use of the NFT media by the copyright owner in relation to NFT buyers, any other contract parties, or other third parties that may have an interest in marketing the NFTs.

Basic NFT buyer rights should present ample opportunities for the buyer to enjoy their NFT, such as displaying it in a metaverse. However, any rights beyond public display or personal use should be carefully considered by the seller before being provided to NFT buyers. For details on intellectual property considerations related to NFTs, see Article, NFTs and Intellectual Property.

Specifying Role of Smart Contracts in the NFT

Smart contract coding and deployment is often a core component of NFT-related agreements. One key issue that parties should consider, and memorialize in contract terms, is whether or not the NFT smart contract should be programmed with a "kill switch" that allows the smart contract code to be altered or updated. In certain circumstances, there may be advantages to programming the smart contract without a kill switch. For example, the absence of a kill switch may provide the market with a higher degree of confidence that the NFT will not be altered post-sale. On the other hand, the ability to alter smart contracts code may offer certain advantages, especially as technology continues to develop and new technical functionality becomes available.

One particular area of relevance relates to securing-perpetual-royalty features. As the open-source coding community continues to find creative ways to improve perpetual royalty functionality, NFT sellers may benefit from being able to implement smart contract upgrades to enhance these capabilities as new techniques are deployed, tested, and validated.

Third-party audit rights are another area that should be considered. Providing for a third-party technical audit of the smart contract code provides assurance that the code functions as intended. The cost of a third-party technical audit and the costs of any work required to correct any identified deficiencies are points of contract negotiation. Similarly, the parties may have an interest in defining certain key smart contract functions and designating responsibilities and remedies in the event a smart contract malfunction occurs.

For further information on smart contracts, see Practice Note, Smart Contracts: Best Practices.

Data Privacy and Security Considerations in NFT Contract Negotiation

Data privacy issues should be carefully considered during NFT contract negotiations. At a minimum, contract terms should address privacy policies and compliance with applicable privacy laws. Depending on the nature of the transaction, additional data privacy issues may need to be negotiated, such as remedies for privacy violations and data breaches, as well as related insurance and indemnification. Security incidents and notification procedures should be clearly defined. In some cases, a separate data privacy and security addendum may be appropriate.

In some cases, technical service agreements involving NFTs may result in the collection and generation of valuable data. In these instances, data privacy provisions must be integrated with provisions that govern the rights of the parties to access, use, and claim ownership of certain data. This data may be especially valuable because the NFT market is so new and reliable market benchmarking data is mostly unavailable. In some instances, one contract counterparty may seek ownership of certain data, but the other counterparty may seek a limited license to use the data in a way that mutually benefits the parties.

The parameters of these arrangements should be evaluated and clearly defined in the contract terms. To the extent that a party is allowed to maintain and use data owned by the other party, the contract terms should articulate standards for anonymizing or deidentifying any data that could be considered personal data under applicable privacy laws.

For further information, see NFTs: Data Privacy and Information Security Considerations.

Accounting for the Digital Millennium Copyright Act (DMCA)

The Digital Millennium Copyright Act (DMCA) provides certain remedies in scenarios where NFTs are created and sold using NFT media in a manner that violates a third party's copyright. NFT marketplaces and other vendors involved in the minting and initial sale of NFTs should have a clear DMCA public notice, as well as an internal DMCA response plan to combat intellectual property violations. DMCA takedown notice procedures and a designated DMCA agent are also required and should be incorporated into terms of use. For more information, see Practice Notes, NFTs and Intellectual Property: Digital Rights Management and DMCA Takedown Requests and Digital Millennium Copyright Act (DMCA): Safe Harbors for Online Service Providers.

Standard Terms May No Longer Be Standard

Similar to the cryptocurrency market generally, the unique aspects of the NFT market call for certain updates to contract clauses that typically govern matters such as termination, indemnification, limitation of liability, and other concepts that are sometimes thought of as boilerplate. With respect to termination, market conditions may call for provisions that reflect the evolving balance of power between different market participants. Indemnification and limitation of liability provisions should address copyright and other relevant intellectual property, technical aspects of decentralized blockchain networks, and other NFT-specific issues.

NFTs: Intellectual Property (IP) Legal Issues

Noteworthy NFT IP Court Cases: MetaBirkin and Bored Ape

Courts recently decided two important cases regarding NFTs and IP:

- *Hermes Int'l v. Rothschild*, No. 1:22-cv-00384 (S.D.N.Y. Feb. 14, 2023). For details, see Legal Update, Jury Finds MetaBirkin NFTs Infringe Hermès' Trademark Rights.
- .*Yuga Labs Inc. v. Ripps*, No. 2:22-cv-04355 (C.D. Cal. April 24, 2023). For details, see Legal Update, Bored Ape NFTs Are Protectable Goods Under the Lanham Act: C.D. Cal..

For a general discussion of IP legal issues relevant to NFTs, see Article, NFTs and Intellectual Property.

For information on contractual considerations related to NFT copyright issues, see Key Issues to Consider in NFT Contract Negotiation.

NFTs in Advertising and Marketing Campaigns

Advertisers have embraced NFTs as a new means of boosting both brand visibility and revenue. The consumer experience of participating in NFT "drops" and secondary market trading has opened new avenues for advertisers to deliver unique brand experiences, interact with and expand their customer base, and generate promotional excitement for an upcoming event or product launch. Additionally, many brands have used the sale of NFTs to generate secondary, often lucrative, revenue streams.

Examples of NFT Campaigns

In an effort to engage audiences and produce secondary revenue streams, brands in sectors ranging from fashion to sports, alcohol to art, music to beauty melded visual media, blockchain technology, and e-commerce to create and market new NFT-based digital brand campaigns for everything from toilet paper to tacos.

Advertisers have not only used NFT campaigns to grant ownership rights in a digital media file, such as an image or a video, but also have included rights to physical items, such as clothing. NFTs that provide access rights to digital media only have been more common, with name brands such as Marvel, Disney, ViacomCBS, Macys, and GAP all entering the NFT market in this manner.

NFTs that offer both digital media file access and the right to a physical item have become more popular. For example:

- Mattel launched an NFT auction for a Barbie-Balmain collaboration featuring unique Barbie avatars adorned in Balmain-designed outfits where the highest bidders also received a physical set of Barbie-sized Balmain pieces.
- Levi's promoted a contest in France featuring a prize that consisted of a pair of limited-edition recyclable 501 Originals to be accompanied by an NFT that allows for free jean repair until 2027.

Several brands have paired the sale of branded NFTs with charitable promotions. In those campaigns, proceeds from

sales of branded NFTs raised funds for various charities. For example:

- Taco Bell released a set of limited-edition taco-themed NFTs to raise money for its Taco Bell Foundation
- Charmin released its NFT to raise funds for Direct Relief.
- Coca-Cola released special edition "loot box" NFTs to raise money for Special Olympics International.

Issues Arising from Using NFTs in Advertising and Marketing Campaigns

Under the Federal Trade Commission's (FTC) truth-in-advertising-principles:

- Advertising mut be truthful and not misleading.
- Advertising must not be unfair.
- Advertisers must have substantiation for their advertising claims before disseminating them.

These principles apply to NFT-based advertising and marketing campaigns, but these campaigns can also raise some unique legal challenges. A major theme raised by these issues concerns ensuring all material terms and conditions related to the ownership of the NFT are disclosed to the recipient clearly and conspicuously to avoid deception and unfairness.

Brand Ownership of Underlying Rights

Prior to minting an NFT, a brand should first determine what rights it owns in and to the underlying media content that constitutes the NFT Media. This analysis should generally follow a traditional analysis of copyright, trademark, and right of publicity issues, but is likely to vary depending on the type of media involved (such as a photo, video, or interactive) and the rights (if any) the brand intends to confer to potential NFT purchasers (see NFTs: Intellectual Property (IP) Legal Issues).

Rights Granted to Consumers

Once a brand has determined what rights it holds in the NFT, it should then determine:

- Which rights it intends to grant to consumer.
- Which rights it intends to reserve for itself.
- How it can clearly and conspicuously communicate to the consumer the rights granted, the rights reserved, and all other material terms and conditions.

These determinations help define the design and execution of the NFT promotion. For example, brands generally want to grant the consumer only a limited license to display the underlying artwork asset for personal use. It is important that consumers know that the purchase of an NFT does not give them the right to:

- Reproduce the work.
- Transform the work.
- Create a derivative work.
- Use the work for commercial purposes.

These restrictions should be clearly and conspicuously disclosed to consumers as they typically do not understand the limitations that come with the acquisition of an NFT.

Brands should also determine whether and how they wish to use their marks in connection with NFTs. Although inclusion of a mark may help raise visibility and brand awareness, it also brings an increased risk of misappropriation and dilution. Brands that use their marks in connection with NFTs should be prepared to increase their monitoring of online marketplaces for potential downstream misuse of a mark.

Royalty Payments

In the physical world, secondary resales of an item do not benefit the original creator. The digital world has changed that paradigm. Due to coding built into smart contracts, digital creators can reap the rewards of the resale of their images potentially in perpetuity. However, it is important that brands clearly disclose to consumers that the mere purchase or receipt of an NFT does not give them the right to receive those secondary market royalties when a future sale of the NFT or its underlying media occurs.

Rights Termination

Brands should also consider the termination of rights conferred to an NFT recipient, especially if the NFT media contains brand-related trademarks and copyrights. Brands may want the option to revoke user licenses if certain conditions are violated. These conditions would not only need to be included in the purchaser terms of use, but also like all other material terms and conditions, may need to be disclosed upfront more clearly and conspicuously. Recipient rights may also be terminated through certain technical controls. For example, if the NFT media is hosted on a cloud account controlled by the seller, the seller may retain the technical capability to delete, alter, or otherwise disassociate the NFT media from the NFT token.

Advertising to Children

Brands from Mattel to Marvel have embraced the NFT marketplace, offering digital wares ranging from Barbie dolls to comic books. Although these items may be designed to tap into nostalgia in adult consumers, it is likely that these kinds of digital offerings may also appeal to children. Companies issuing NFTs appealing to children under 13 are likely subject to the Children's Online Privacy Protection Act (COPPA) and a growing set of state laws, some protecting children up to 18.

Advertisers should ensure that all companies involved in interacting with children or handling children's personal information in an NFT campaign have taken appropriate compliance measures (see Protecting Children and Their Personal Information).

NFTs as Part of a Cause Marketing Campaign

All cause marketing promotions are subject to generally applicable advertising and marketing laws, but certain cause marketing campaigns, known as commercial co-ventures, are subject to additional state regulations. Commercial co-ventures are a subset of cause marketing that typically involve consumers making purchases from a for-profit company to benefit a charitable cause. Often, this type of cause marketing looks like a company donating a portion of the sales of a product to charity.

Many states regulate the use of commercial co-ventures to protect consumers from false or misleading sales promotions and ensure that the designated charity actually receives its share of the proceeds that the commercial co-venturer commits to donating. These laws impose different obligations, such as registration and disclosure requirements, that companies must consider when developing their programs.

If a company sells an NFT to raise money for a charity these commercial co-venture laws may apply. For more information, see Practice Note, Cause Marketing: Commercial Co-Ventures and Cause-Related Marketing by For-Profit Companies: Commercial Co-Venturer Checklist.

NFTs as a Sweepstakes or Contest Prize

Sweepstakes and contests (prize promotions) are governed primarily by a patchwork of state rules and regulations that continue to apply when NFTs are offered as a prize. Except for permitted state-run lotteries, these rules and regulations prohibit lotteries. Companies must therefore structure prize promotions to avoid being deemed an illegal lottery. A lottery is comprised of three elements:

- Prize.
- Chance.
- Consideration.

By eliminating any one of these elements, prize promotions can avoid becoming an illegal lottery. Sweepstakes typically eliminate consideration and contests typically eliminate chance. For more information on conducting lawful prize promotions, see Practice Note, Running a Sweepstakes or Contest in the US.

State laws and regulations require companies conducting prize promotions to establish and publish official rules. Prize promotions involving NFTs and the transfer of cryptocurrencies must be mindful of unique elements inherent in the blockchain sphere that may need to be disclosed in official rules. For example, official rules of any prize promotions offering an NFT as a prize should:

- Require that winners (rather than all participants) have a digital wallet to accept the NFT prize and advise that winners are responsible for bearing the cost of any digital wallet fees.
- Clearly and conspicuously disclose that the value of the NFT may fluctuate due to market volatility by:
  - setting a fixed date for the prize valuation;
  - disclaiming liability for any potential loss of value; and
  - establishing a firm date by which tax liability will be established.
- Clearly and conspicuously disclose the winner's rights to and limitations on their use of the NFT by:
  - informing participants what winners can and cannot do with the underlying media file(s);
  - informing participants that winners are not eligible to participate in any royalties that may stem from future sales of the NFT; and
  - disclaiming liability for any future inability of the winner to access the underlying media files connected to the NFT resulting from either technological issues (including hacks) or changes in legal or regulatory regimes.

Considerations in Advertising and Marketing of NFTs

Advertising and marketing an NFT should comply with basic advertising principles, typically enforced by the

Federal Trade Commission (FTC) under Section 5 of the FTC Act, including:

- Advertisements must be truthful and not misleading.
- Advertisements cannot be unfair.
- Advertisers must have evidence to substantiate the claims made in their advertising prior to disseminating the advertising.
- Advertisers must present all disclosures that are required to prevent an advertisement from being misleading clearly and conspicuously.

Because purchasing and owning and NFT is more complex than purchasing and owning tangible items, like consumer packaged goods, advertisers need to be extra cautious to clearly and conspicuously disclose all material terms and conditions of purchasing an advertised NFT and the rights ownership entails. For example, if an NFT is advertised as a limited edition, it must truly be a limited edition. A material disclosure might be the number of editions minted and that disclosure must then appear clearly and conspicuously near the limited edition claim. For more information on advertising principles, see Practice Notes, Advertising: Overview and Advertising Claim Fundamentals.

Advertisers must also consider some additional issues when advertising NFTs on social media, for example:

- Social media platform advertising guidelines.
- Restrictions on influencer marketing.

Social media platforms often prohibit the advertising and sale of certain items and those prohibitions may apply to cryptocurrencies and NFTs. Before advertising an NFT on any social media platform, check its guidelines for any prohibition that could encompass advertising the sale of NFTs. In addition, as social media platforms may adapt their guidelines regularly, guidelines should be checked before launching every new advertising campaign.

Before engaging in any influencer marketing, NFT advertisers should comply with FTC guidance on influencer marketing, including, most importantly, the FTC's Guides Concerning the Use of Endorsements and Testimonials in Advertising (Endorsement Guides) (16 C.F.R. §§ 255.0 to 255.5), which the FTC recently updated in June of 2023. Under the Endorsement Guides and other FTC guidance, to mitigate the risk of conducting deceptive influencer marketing, advertisers should:

- Ensure all influencer posts include a clear and conspicuous disclosure about the material connection between the influencer and the advertiser.
- Ensure influencer posts do not contain any unsubstantiated claims about the advertiser's products or services.
- Require influencer posts be based on the influencer's honest opinions, beliefs, experiences.
- Train employees, agencies, and influencers on FTC guidance.
- Monitor influencer posts to ensure compliance with disclosure requirements and other requirements under the Endorsement Guides.
- Take corrective measures to address failures by influencers to comply with the Endorsement Guides.

The Securities Act also sets out a requirement that influencers posting about NFTs may need to follow depending on whether the NFT is viewed as a security. Section 17(b) of the Securities Act makes it unlawful for any person to promote a security without fully disclosing the amount paid for the post (see Legal Update, SEC Settles Charges Against Kim Kardashian for Unlawful Touting of Crypto Assets).

For more information on influencer marketing, see Practice Note, Social Media Influencer Marketing: Practical Tips for Managing Legal and Reputational Risks.

NFTs: Data Privacy and Information Security Considerations

NFT service providers and ecosystem participants are subject to the same general and sector-specific federal and state data privacy and information security laws that apply to any organization that handles personal information. The characteristics of an NFT service provider's or ecosystem participant's business operations and the NFTs that they service are critical factors in determining whether and how data privacy and information security laws apply. For example, when reviewing data privacy and information security laws, NFT service providers and ecosystem participants must consider factors that include:

- Their role, specifically – whether they have a direct relationship with consumers or other individuals or service companies that do, or both.
- The types of personal information and other data that they collect and manage and where individuals reside and interact with their services.
- How the NFT platforms they operate and use are implemented, including the locations where they store and manage personal information.

- Whether sector-specific laws and regulations or exemptions apply to them.

Some examples of federal and state laws and regulations that may apply include:

- Broad consumer protection laws, such as the Federal Trade Commission (FTC) Act, which are not specifically data privacy and information security laws but are used to prohibit unfair or deceptive practices in the collection, use, processing, protection, and disclosure of personal information (for more information, see Practice Note, FTC Data Security Standards and Enforcement and FTC Data Security Actions Tracker).
- Sector-specific laws relevant to particular industries, including:
  - the FTC's Red Flags Rule, issued under the Fair and Accurate Credit Transactions Act, which requires financial institutions and creditors with covered accounts to develop a written program that identifies and detects relevant warning signs (or red flags) of identity theft (see Standard Document, Red Flags Rule Identity Theft Prevention Program Master Policy)
  - the FTC's Safeguards Rule, issued under the Gramm-Leach-Bliley Act (GLBA), which requires non-banking financial institutions to develop, implement, and maintain a written information security program to protect customer information and notify the FTC under certain circumstances when unauthorized data acquisitions occur.
  - the cybersecurity regulation issued by the New York State Department of Financial Services, which similarly requires BitLicense holders and other licensees to develop, implement, and maintain a written information security program and notify the DFS under certain circumstances when a security incident occurs.
  - the Children's Online Privacy Protection Act (COPPA) and a growing set of state laws, if the NFT service provider's or ecosystem participant's products and services appeal to children (see Protecting Children and Their Personal Information).
- State-level laws such as:
  - biometrics data privacy laws that protect human biology measurements and behavioral characteristics, such as facial geometry, iris scans, voiceprints, and fingerprints, which an organization can use to identify a specific individual;
  - broad consumer data privacy laws, which a growing set of states have enacted or are considering, including California, Colorado, Connecticut, Delaware, Indiana, Iowa, Montana, Oregon, Tennessee, Texas, Utah, and Virginia, although they generally include various exemptions for those subject to sector-specific and certain other laws (for details on these and other state data privacy and information security laws, including a state-by-state listing of resources, see State Data Privacy Laws Toolkit);
  - data breach notification laws, which require organizations to notify affected individuals and authorities under certain circumstances when breaches of personal information occur; and
  - data security laws, which impose obligations on organizations to protect the personal information they hold from unauthorized access, use, or disclosure.

US businesses that operate multi-nationally must also consider the data protection laws in each jurisdiction in which they operate. For example, the EU imposes extensive obligations under its General Data Protection Regulation (GDPR). For details in GDPR, see GDPR Resources for US Practitioners Toolkit. NFT service providers and ecosystem participants should review the same factors to determine which local laws and regulations may apply for each relevant jurisdiction.

The data privacy and information security obligations of NFT service providers depend on what they control – namely, their own databases and information systems relating to the NFT transactions that they service. These obligations are further determined by the service providers' own business practices and the types of NFTs that they service. For example, minters, exchanges, and custodians interact directly with NFTs and NFT holders, but media file managers generally do not. These parties therefore each have different data protection obligations.

NFT platforms, like many blockchain applications, also face certain unique challenges in defining personal information and assessing regulatory compliance needs and risks, including issues around anonymity and pseudonymity, territorial considerations, and cross-border data transfers. For details on recognizing and managing these risks, see Practice Note, Blockchain Technology: Data Privacy Issues and Potential Mitigation Strategies.

NFT service providers and ecosystem participants should also consider the cybersecurity risks that exist in any blockchain application, such as:

- Transaction data and validation risks and potential blockchain integrity attacks.
- Dependencies on external data or other at-risk resources.

- The cyber vulnerabilities that may exist in:
  - a blockchain application's implementing code, including the NFT platform's code;
  - the environment in which the technology runs; and
  - end-user environments, especially wallets and the options consumers have for protecting them.

Information stored on the blockchain is typically minimal in nature (for example, digital asset identification, transaction consideration, time stamp, and public keys) and generally does not include personal information because storing information on-chain is costly, cumbersome, and in the public domain. However, this on-chain information may be connected to personal information located in the databases of service providers through a user's public key. This connection creates data privacy and information security issues that NFT service providers must address.

Both the US Treasury Department and the Financial Action Task Force (FATF) have indicated that, depending on their nature and characteristics, certain NFTs may be deemed convertible virtual currency (CVC) if they are used for payment or investment purposes (see NFTs: Anti-Money Laundering (AML) and US Economic Sanctions). Therefore, service providers of payment or investment NFTs likely are subject to various financial services laws that require:

- The collection of personal information of persons transacting in these NFTs.
- The disclosure of their information-collection practices to NFT holders.
- The implementation of safeguards to protect this information.

Additionally, most NFTs point to a media file (image, video, or .gif) through a uniform resource identifier (URI). This off-chain media may be in the form of an image, video, or audio file that may also include personal information depending on the function of the NFT. While NFTs for artwork, collectibles, and music likely do not contain personal information, other use cases for NFTs relating to identity and ownership may contain personal information posing data privacy issues.

For more information on blockchain cyber risks and related issues, see Practice Note, Cybersecurity Tech Basics: Blockchain Technology Cyber Risks and Issues: Overview.

Protecting Children and Their Personal Information

Companies issuing NFTs that target or are appealing to children under 13 are likely subject to the COPPA and a growing set of state laws. COPPA applies to websites and other online services designed for:

- Children under 13.
- General audiences that knowingly collect personal information from children under 13.

Under COPPA, these websites and online services must protect children's personal information by taking a number of steps, including:

- Providing clear and conspicuous notice of the information collected, how the operator uses that information, and how that information is shared.
- Obtaining verifiable parental consent for the collection, use, and disclosure of personal information from children.
- Retaining collected information for only as long as is needed to perform the disclosed task.
- Providing parental access to the collected information along with a method for deletion, if requested.
- Safely and securely handling the collected information and treating it as confidential.

For more information on COPPA compliance, see Practice Note, Children's Online Privacy: COPPA Compliance.

A growing set of states have also enacted or are considering laws that set online standards for protecting children and their personal information and may apply to NFT service providers and ecosystem participants. For example:

- The California Age-Appropriate Design Code Act:
  - imposes new legal obligations on companies that provide online services, products, or features that children under 18 are likely to access; and
  - takes effect July 1, 2024.

  (Cal Civ. Code §§ 1798.99.28 to 1798.99.40; for more information, see Practice Note, California Privacy and Data Security Law: Overview: Age-Appropriate Design Code Act.)
- The Utah Social Media Regulation Act:

- imposes various obligations on certain social media platforms to protect children under 18; and
- for most provisions, takes effect March 1, 2024.

(See Legal Update, Utah Enacts Social Media Regulation Act.)

NFT service providers and ecosystem participants that operate in non-US jurisdictions must also recognize that global data protection laws vary in how they treat children and the age thresholds that they set.

NFTs: Anti-Fraud and Anti-Corruption

NFT market participants should understand fraud risks in the NFT market and take steps to protect themselves from becoming victims of fraud, or unwittingly facilitating fraud.

Protecting Against Counterfeit NFTs

As noted above, the value of an NFT is generally derived from the NFT media, its rarity and authenticity, as well as the identity of the associated artist. The NFT authenticates the NFT media, in many respects, by proving that the NFT media was attached to the NFT by a specific person at a specific point in time. However, the NFT media cannot authenticate the NFT. According to reports, certain counterfeiters have therefore downloaded an image of an artist's work and used it to mint and sell NFTs without permission from the actual artist. Typologies where counterfeiting has begun to emerge in the NFT market include:

- Minting NFTs using another artist's work (sometimes with slight changes).
- Copying certain source code used to generate NFT media and using it without permission.
- Creating fake websites that redirect NFT purchase payments from legitimate websites.
- Exploiting vulnerabilities on an artist's legitimate website to post counterfeit NFTs for sale.

Many NFT marketplaces place the burden of identifying and reporting counterfeit NFTs on the artists themselves. However, NFT marketplaces should consider implementing additional mechanisms to combat counterfeit NFTs, including:

- Maintaining a database of artist work that is already posted on the platform, using image-matching technology to scan new NFTs against the database for similar images, and notifying artists when their images have been minted as new NFTs.
- Implementing due diligence procedures to verify NFT sellers' accounts and creating a system to notify buyers that the art sold through that account is verified as authentic.
- Creating a shared register of known instances of art that has been used in counterfeit NFTs to alert other platforms to conduct heightened due diligence on the seller attempting to sell NFTs using such art.
- Scanning for embedded digital signatures, watermarks or fingerprints, or employing technology that assesses the rarity of the underlying pixel patterns of the NFT media.

Buyers can also protect themselves by:

- Analyzing the websites that purport to be "official" NFT stores for artists or brands.
- Researching whether certain brands or artists have sponsored campaigns or released official commentary regarding which platforms are official sellers of their artwork.
- Monitoring whether the artist or platform has released information regarding the numbers of NFTs that have been officially minted for sale and how many have been sold to date.

Preventing Insider Trading of NFTs

Insider trading on NFT marketplaces is a serious risk. For example, employees may use insider information to purchase exclusive NFTs before they are available to the public, and later sell for a profit when prices spike. Insiders may also provide sensitive information regarding surprise drop times or use their permissions to grant early access to friends and family. This is what occurred in the two major NFT insider trading cases to date on the Coinbase and OpenSea platforms. For details on these, see NFT Insider Trading Cases.

Some steps NFT marketplaces can take to prevent insider trading include the following:

- **Formal policies.** Implementing a written policy that prohibits the use of insider information, defines "insider" and "insider information," and clearly articulates prohibited conduct.
- **Training.** Educating employees regarding what constitutes insider information and its inappropriate uses and communicating the consequences of insider trading.

- **Monitoring.** Creating an internal watchdog position to oversee and review NFT purchases and sales by marketplace insiders.
- **Controls.** Implementing controls, such as requiring permission in instances where employees seek to buy or sell NFTs, and implementing technology to automatically flag transactions by insiders for review.
- **Reporting.** Requiring employees to periodically submit a list of their cryptocurrency accounts and the NFTs they own with attestations that the NFTs were bought with publicly available information. NFT marketplaces should consider restricting employee trading only to identified accounts and take corrective and disciplinary action against employees trading using unreported accounts.
- **Blackout periods.** Restricting employee transactions in certain NFTs sold on the NFT marketplace at specific times, such as the weeks around particular NFT drops.
- **Hotlines.** Providing anonymous reporting lines for employees to share information and quickly investigating insider trading tips.
- **Firewalls.** Separating duties or creating informational walls between employees responsible for preparing NFTs for launch and departments related to sales.

NFT Market Manipulation

Like any other asset for which there is a marketplace, NFTs may be subject to the following types of market manipulation:

Spoofing and Shill Bidding of NFTs

Spoofing occurs when a fraudster creates a high volume of fictitious buy or sell orders that tricks average traders into thinking large or high-volume transactions are occurring. Average traders rush to do what they believe the market is doing, often being coerced into selling cheap or buying high to create more favorable conditions for the fraudster. Once the market moves, the fraudster cancels the fictitious order(s). Spoofing is often executed using algorithms and bots.

In the NFT context, spoofing can occur when a fraudster uses dummy accounts to place large volumes of low bids on NFTs to coerce the seller to sell at a lower price. Once a bid is accepted, the fraudster cancels the order and the seller must relist it, but the low bid creates a new price floor and the fraudster then uses another account to purchase at the lower price.

A similar technique is shill bidding. This is where the fraudster uses another account or has family and friends bid on their NFT to artificially drive up the price. Spoofing and shill bidding rig the market to the detriment of honest buyers and sellers.

Wash Trading of NFTs

Wash trading occurs when a fraudster opens multiple accounts and conducts a series of trades among those accounts to create artificial pricing and trading volume. The NFT is then sold to traders who think the artificial prices and buyer interest will continue. Another wash trading scenario occurs when an NFT seller mints an NFT and sells it to themselves for a specific price to create artificial market demand. The seller then sells the NFT to another buyer for a significantly lower price, making it seem as if the buyer is getting a good deal, but the entire value was artificially created.

NFT Pump and Dumps

NFTs are also susceptible to classic pump-and-dump schemes. In the NFT context, traders use social media to rally attention around the NFTs and "pump-up" demand and the price. The traders then "dump" (sell) the overvalued assets for a profit, and the NFT price falls once the NFTs are in the hands of honest buyers.

Combating NFT Market Manipulation

NFT marketplaces should consider implementing automated monitoring tools to identify potential market manipulation risks. These tools can perform functions, including:

- Detecting bot bid activity, such as when:
  - a larger number of bids are being placed than are manually possible; or
  - a pattern of large orders and audit cancellations occur related to specific accounts or NFTs.
- Flagging transactions where the chain of custody ends with the same person who initiated the sale.
- Identifying suspicious activity among accounts of related individuals.
- Notifying marketplace users watching an NFT when a sold NFT ends up with the same seller.

NFT buyers can also take steps to protect themselves, including:

- Learning how to identify spoofing and shill bidding patterns, including bidding-and-cancellation activity.
- Watching for bidders immediately outbidding them every time and reviewing orders placed during the

previous few days to identify whether reorders suddenly change or disappear on a regular basis.

- Tracing NFTs that were traded at a rapid pace and suddenly stopped, to identify any connection between the original seller and user NFT wallets or accounts.
- Identifying users that buy and re-sell NFTs among themselves.
- Limiting participation to NFT marketplaces that use automated systems to prevent market manipulation and that take other steps to prevent fraudulent activity.
- Recognizing that order books that appear too good to be true likely are.

NFT FCPA and Bribery Considerations

The Foreign Corrupt Practices Act (FCPA) makes it a crime to make a payment, offer or promise to pay, or authorize a payment of money or anything of value, directly or indirectly, to any foreign official, politician, party official, candidate for office with a corrupt intent for the purpose of influencing the person's official acts or decisions in violation of their lawful duty to obtain or retain business. While under-the-table cash payments represent the classic example of bribery, the FCPA prohibits the payment of anything of value, which includes gifts of NFTs or sensitive information regarding upcoming sales of NFTs, or the payment of cryptocurrency to fund purchases of NFTs.

Companies with FCPA compliance programs should update those programs to address cryptocurrency and NFT-related FCPA risks. Some examples include the following:

- **Disclosures.** Updating due diligence and risk assessments on third-party entities and their principals to require disclosure of active crypto and NFT activity, including statements of purpose and industry connection.
- **Explicit prohibitions.** Explicitly referencing crypto assets, including NFTs, as forms of prohibited payments or gifts to foreign officials that can subject employees to corrective or disciplinary action.
- **Training.** Providing periodic anti-corruption compliance training and education to employees regarding the specific types of crypto-asset transactions, including those involving NFTs, that violate the FCPA and requiring annual certification of compliance with FCPA.
- **Reporting.** Implementing a periodic employee questionnaire inquiring whether employees own crypto assets, including NFTs, whether they use company devices to access crypto accounts or NFT platforms, and whether they have conducted crypto-asset transactions, including those involving NFTs, in high-risk jurisdictions.
- **Permissions.** Defining the employees within the company with permission to conduct business in crypto assets, including NFTs, which wallet addresses are permitted for corporate use, and which persons may receive payments in connection with these crypto assets.
- **Monitoring.** Implementing procedures to monitor traditional company bank accounts for transfers that involve the purchase of NFTs or other crypto assets.
- **Hotlines.** Establishing anonymous reporting mechanisms to collect information regarding possible or solicited bribes, educating employees on how to report bribes that take the form of NFTs or other crypto assets, and quickly investigating potential violations.

NFT Fraud Typologies

Fraud schemes involving NFTs operate like any other fraud scheme – a person is deceived into parting with something of value and receives little to nothing in return, to the enrichment of the fraudster. NFT fraud schemes may be advertised on social media platforms to rally attention, marketed with websites that appear legitimate, and even employ online chat-function technology to lure victims. Examples of fraud typologies that may arise in the NFT market include the following:

- **Fraudulent NFT sales.** A fraudulent NFT seller never delivers the NFT to the buyer or delivers something not promised.
- **Fraudulent inducement.** A fraudster contacts a vulnerable victim, such as an elderly individual or someone with no cryptocurrency experience, and uses a scheme to convince the victim into completing an NFT or cryptocurrency transaction that inures to the benefit of the fraudster. Examples of schemes fraudsters may use include impersonating a friend or family member, purporting to represent a legitimate enterprise (including an NFT trading platform), romance scams, or fake contest prizes.
- **Investment schemes.** A fraudster claims they manage an investment vehicle to pool assets and invest in NFTs. The victim invests in the form of cryptocurrency, and the fraudster absconds with funds. Alternatively, when the victim tries to make a withdrawal, the victim is asked to pay "withdrawal fees" to withdraw their assets.
- **Ponzi schemes.** A fraudster claims to manage NFT investments and perpetuates an investment scheme that promises high and quick returns. When a victim

requests to cash out the value of their NFT "profits," they are paid with the cryptocurrency of other investors.

NFT market participants can defend against fraud by conducting due diligence on NFT sellers and other third parties, and by watching out for common signs of fraud, including:

- Typographical errors and obvious misspellings in emails, social media posts, or other communications.
- Promises to multiply the investment.
- Promises of free money.
- Secretive or complex strategies and fee structures.
- Fake influencer or celebrity-led social media campaigns.
- Reluctance to grant access to account information.
- Errors in account statements.

NFTs: Applicable Anti-Money Laundering (AML) Rules and Considerations

Applying US AML Regulations to NFTs

The primary tools that the US government uses to fight money laundering and terrorism financing are the Bank Secrecy Act (BSA), related federal AML laws, and related regulations promulgated thereunder by the US Treasury Department's Financial Crimes Enforcement Network (FinCEN) (collectively, the BSA provisions). Among other things, the BSA provisions place registration, recordkeeping, and AML reporting obligations on entities that qualify as money services businesses (MSBs). For details on which crypto businesses may be MSBs under the BSA provisions, see Practice Note, FinCEN Regulation of Virtual Currency: Overview: Application of FinCEN's Regulations to Certain Business Models Involving CVC.

NFTs often involve two areas with known money laundering and terrorist financing risks, cryptocurrencies and high-value assets, like art. Auction houses that have traditionally operated in the physical art space but have since incorporated NFTs into their inventory are subject to reporting requirements as financial institutions under the BSA, as amended by the Anti-Money Laundering Act of 2020 (AMLA). In certain circumstances, other NFT market actors may be subject to the BSA, as well.

The BSA provisions are designed to help law enforcement and the US government identify and deter financial crimes, and NFTs share qualities of convertible virtual currency (CVC), as defined by FinCEN, as well as certain high-value assets, such as art and gemstones, that already draw increased AML attention from regulators. Accordingly, while the BSA provisions do not explicitly address NFTs, they may be applied to NFTs using existing guidance. From a practical perspective, the application of the BSA provisions to the NFT market will likely be determined on a case-by-case, fact-specific basis. Additionally, due to overlap of NFT characteristics with those of CVCs and other high value assets, additional AML regulations or guidance addressing NFTs may be forthcoming.

As detailed below, FinCEN has provided guidance on the application of statutes related to AML and the countering of terrorist financing (AML-CTF) to cryptocurrencies – specifically convertible virtual currency, or CVC. FinCEN defines CVC broadly. For details on the FinCEN CVC definition, see Practice Note, FinCEN Regulation of Virtual Currency: Overview : FinCEN Definition of Convertible Virtual Currency (CVC).

Are NFTs Convertible Virtual Currency (CVC) Subject to FinCEN Rules?

Whether an NFT may be considered CVC, subjecting certain parties transacting in them to FinCEN regulations, remains an open question. In general, based on FinCEN guidance, it appears that whether an NFT qualifies as a CVC turns on whether, if examined by FinCEN, the NFT would be deemed to be "value that substitutes for currency."

On one hand, the Financial Action Task Force (FATF) guidance seems to indicate that NFTs should not be considered "value that substitutes for currency" (see Application of Financial Action Task Force (FATF) Guidance to NFTs). On the other hand, the February 2022 study published by the US Department of the Treasury on the facilitation of money laundering and terror finance through the trade in works of art indicated that, depending on their characteristics and how they are used, certain NFTs may fall within the CVC definition.

The question of whether NFTs meet FinCEN's definition of CVCs is critical for NFT marketplaces and other business models that facilitate the minting, initial sale, and secondary trading of NFTs. These businesses should conduct a careful analysis of their specific activities and the specific NFTs they support to determine whether they would be considered a CVC administrator or exchanger – and therefore an MSB – if examined by FinCEN. Among other things, NFT marketplaces and related businesses should specifically

analyze whether their facilitation of CVC payments in NFT sales creates MSB obligations. Additionally, NFT marketplaces and related businesses should analyze whether the integral exemption or other exemptions are available to exempt their NFT activities – or at least certain aspects of their NFT activities – from MSB obligations.

Identifying and Mitigating NFT-Related AML Risks

Violations of FinCEN regulations carry both civil and criminal penalties. To avoid potential issues, the best practice is for those minting, selling, trading, or in custody of NFTs to work under the assumption that BSA provisions may apply. In this regard, NFT market participants should:

- **Work with registered MSBs wherever possible.** The best practice is to engage a registered MSB to handle all NFT transactions, especially the acceptance and transmission of cryptocurrency and the hosting of NFT-storing wallets. When working with MSBs, confirm that they have implemented an AML program that covers NFT transactions, including potential royalty payments that may be made on subsequent sales.
- **Understand and apply MSB exemptions.** The NFT market is multi-faceted and constantly evolving. Invest the time and effort into understanding the exemptions to the MSB definition and how those exemptions apply to the cryptocurrency space. Analyze NFT market activities and identify whether and where certain exemptions are available.

For further information on FinCEN regulation of crypto assets, see Practice Note, FinCEN Regulation of Virtual Currency: Overview.

Application of Financial Action Task Force (FATF) Guidance to NFTs

In October 2021, the Financial Action Task Force (FATF), an intergovernmental organization designed to combat money laundering and terrorist financing, published Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers (see Legal Update, Updated Version of FATF Guidance on Virtual Assets and Virtual Asset Service Providers: October 2021). While the guidance is not binding on the US, the US is a FATF member nation. The guidance is therefore persuasive, and underscores the need for countries, virtual asset service providers (VASPs), and other entities involved in virtual asset activities to both understand and mitigate money laundering and terrorist financing risks. The guidance also provides specific examples of risk indicators that should be considered in a virtual asset context, with an emphasis on identifying factors that might obfuscate transactions or inhibit the ability of VASPs to properly diligence customers.

The guidance arguably calls for a presumption that NFTs are not virtual assets, due largely to the fact that they are nonfungible:

> "Digital assets that are unique, rather than interchangeable, and that are in practice used as collectibles rather than as payment or investment instruments, can be referred to as non-fungible tokens (NFT) or crypto-collectibles. Such assets, depending on their characteristics, are generally not considered to be virtual assets under the FATF definition."

(Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers.)

The guidance, however, opens the door for FATF members to regulate NFTs as virtual assets if the NFTs are used for payment or investment purposes and concludes that regulators consider the application of the FATF standards to NFTs on a case-by-case basis.

Deterring NFT-Based Money Laundering

There is a risk that the NFT market could enable a new form of digital trade-based money laundering, in which NFTs are used to store, move, and obfuscate the source of funds derived from illegal activity. Even in the absence of a legal/compliance risk, there are business and reputational risks that NFT market participants should consider. For this reason, regardless of their BSA obligations, NFT marketplaces and related businesses should consider implementing programs to detect and prevent the use of NFTs in money laundering. Some measures to consider include the following:

- **Information collection and sharing.** Creating registries of stolen or fraudulently purchased NFTs, and high-risk persons or NFT wallets/public keys, and making these registries accessible to other NFT ecosystem participants.
- **Customer due diligence.** Implementing policies to collect customer information, including official government identification documents, to conduct customer due diligence, combat anonymity, and identify high-risk customers.
- **Transaction monitoring.** Applying automated systems and data analytics to detect potentially suspicious activity, such as high-frequency transactions in

large sums from many accounts to buy a single NFT, consecutive high-value buying and selling of NFTs in a short period of time, wallets that do not match customer profiles, wallets involved in transactions exceeding a certain threshold, and periodic testing to assess whether new controls are needed.

- **Written policies.** Implementing a written AML policy, including procedures for internal reporting, documenting and investigating potential money-laundering, and training for employees to recognize potentially suspicious activity.

Application of US Economic Sanctions to NFTs

Unlike FinCEN regulations, which apply only to certain entities, OFAC regulations apply to all US citizens and lawful permanent residents, as well as all entities organized or substantially operating under the laws of the US. Whether an NFT is a CVC is irrelevant under OFAC. The key issue is whether any transaction – regardless of currency or denomination – occurs with a sanctioned party. OFAC regulations apply to NFT transactions just like any other commercial activity.

The application of OFAC's policies to the crypto space has been evident in its enforcement activity. For example, in November 2021, OFAC sanctioned a Latvia-based cryptocurrency exchange, its associated support network, and two ransomware operators for facilitating financial transactions for ransomware actors. OFAC designated the exchange and 57 cryptocurrency addresses associated with certain related digital wallets as Specially Designated Nationals (SDNs), adding them to OFAC's SDN list. According to reports, the addresses listed by OFAC held 42 NFTs reportedly worth $531,600 at the time (see Legal Update, OFAC Adds Russian-Based Crypto Exchange SUEX OTC and Related Parties to Specially Designated Nationals (SDN) List Over Ransomware Attacks).

Because US persons are prohibited from transacting with individuals and entities associated with the SDN-designated cryptocurrency addresses, any interaction or trade involving the NFTs held by the listed addresses is also prohibited. For further information on OFAC regulation of crypto assets, see OFAC Economic Sanctions: Cryptocurrency and Blockchain.

Identifying and Mitigating NFT-Related OFAC Risks

Violations of OFAC regulations carry both civil and criminal penalties. The NFT market is borderless, and blockchain transactions are pseudo-anonymous. This puts NFTs at higher risk of OFAC violations than in traditional commercial markets. Parties may mitigate this risk by ensuring policies, procedures, and technical controls are in place to prevent transactions with OFAC sanctioned countries or persons on the OFAC SDN List.

NFTs as Commodities Subject to CFTC Regulation

NFTs that are not a digital representation of value that functions as a medium of exchange, a unit of account, and/or a store of value, are unlikely to be deemed virtual currency regulated by the CFTC. If an NFT simply denotes ownership or title, that is also unlikely to be considered a commodity. Similarly, if an NFT is unquestionably a security for capital-raising purposes, it is less likely to be considered a commodity regulated by the CFTC (see below, NFTs Under the US Securities Laws). While the SEC and CFTC share jurisdiction over derivatives on securities, the CFTC's jurisdiction is more expansive over non-security commodities.

However, if an NFT is offered on a margined or leveraged basis, or as part of a futures- or derivatives-type product, then the CFTC regulatory regime is likely to apply. Additionally, spot market activity is subject to CFTC enforcement action for fraud and manipulation, and the CFTC may regulate platforms where NFTs trade.

There have been no CFTC enforcement or regulatory actions to date directly targeting NFTs or NFT exchanges, service providers, or creators. However, CFTC enforcement activity in the crypto space and against crypto exchanges and platforms has been extensive. In particular, consistent with its legislative and judicial authority, the CFTC has focused on:

- Operation of unregistered crypto asset derivatives exchanges.
- Margining retail commodity transactions using cryptocurrency (usually bitcoin).
- Fraud in interstate commerce in the underlying spot commodity (bitcoin, ether) markets.

(See Practice Note, Cryptocurrency and Virtual Currency Regulatory Tracker: Virtual Currency and Cryptocurrency Regulatory Tracker: US Federal.)

To date there has been no indication from the CFTC or otherwise that an NFT would or could be considered a derivatives product though it is not hard to imagine an NFT product that could have some characteristics of a derivative. In any event, CFTC authority over NFTs and NFT platforms could apply in the contexts noted above.

NFTs Under the US Securities Laws

One of the fundamental legal questions surrounding NFTs is whether they are or can be securities requiring registration under or an exemption from the US securities laws. The debate as to whether NFTs are or may be securities under the US securities laws is the same as with any other crypto-asset. Although there are important technical differences between NFTs and other blockchain tokens, the SEC has indicated that it intends to analyze NFTs using the same analysis that it previously applied to the initial coin offering (ICO) market.

The SEC has interpreted the securities laws and regulations strictly with respect to fungible blockchain-based tokens (for example, ERC-20 tokens), finding that many are securities, while at the same time recognizing that a fact-based approach is required (see Practice Note, SEC Regulation of Digital Assets). While there have been requests for the SEC to issue guidance on the application of securities laws to NFTs, to date, neither the SEC nor the staff have issued any such guidance.

In the absence of specific guidance, commentators generally apply the analysis under *Securities and Exchange Commission v. W. J. Howey Co.*, 328 U.S. 293 (1946) to all tokens and digital assets, including NFT projects, to determine whether an investment contract has been formed, creating a security under the US securities laws. The *Howey* analysis includes the following prongs:

- An investment of money (see Applying Howey Prongs to NFTs: Investment of Money).
- In a common enterprise (see Applying Howey Prongs to NFTs: Common Enterprise).
- With a reasonable expectation of profits based on the efforts of others (see Applying Howey Prongs to NFTs: Reasonable Expectation of Profits Based on the Efforts of Others).

(See Howey Test Flowchart.)

For digital assets, including NFTs, the *Howey* analysis is conducted through the lens of the SEC's April 2019 Framework for "Investment Contract" Analysis of Digital Assets (SEC framework).

Application of *Howey* Test to NFTs

Applying *Howey* Prongs to NFTs: Investment of Money

A purchaser buying an NFT using fiat or cryptocurrency would satisfy the first prong of the *Howey* test – an investment of money. If a purchaser obtains the NFT by other consideration, this would require a facts-and-circumstances analysis as to whether the purchaser is giving up specific consideration in return for a separable financial interest with the characteristics of a security and whether that consideration is "tangible and definable." In addition, labor or giving up resources may, in certain circumstances, be considered an investment of money (*Uselton v. Commercial Lovelace Motor Freight, Inc.*, 940 F.2d 564 (10th Cir. 1991); but see *Int'l Brotherhood of Teamsters v. Daniel*, 439 U.S. 551 (1979)).

For further information on this *Howey* prong, see Practice Note, Security Defined: Investment of Money.

For further information on the application of *Howey* to crypto assets, see Practice Note, SEC Regulation of Digital Assets: SEC Approach to Digital Asset Regulation: Howey Test and FinHub Framework.

See also, Practice Note, Security Defined: Cryptocurrencies and Digital Assets.

Applying *Howey* Prongs to NFTs: Common Enterprise

Whether the offer and sale of an NFT satisfies the common enterprise prong – often referred to as the commonality prong – depends on the:

- Use of the proceeds from sale of the NFT.
- Bundle of rights associated with the NFT.
- Manner in which the NFT is minted, distributed, and sold.

For example, the common enterprise (vertical or horizontal) prong is more likely to be met when the proceeds of an NFT sale are pooled together and used to build a platform or network associated with the NFT. Similarly, if purchasers receive some sort of pro-rata distribution of profits, commonality (horizontal) is more likely to exist. If the NFT purchasers depend on the efforts of a promoter, or the collective success of the purchasers and promoter are connected, there is more likely to be a common enterprise (vertical).

NFTs that have the characteristics of fractionalization (F-NFTs), as well as royalty payments associated with F-NFTs, are likely to receive more scrutiny regarding whether a common enterprise exists, because they involve aspects akin to pooled resources. When an NFT is fractionalized, the fractionalized tokens are typically fungible tokens that comprise the non-fungible token and must be analyzed accordingly (see Fractionalized NFTs (F-NFTs)).

In the case of art NFTs, the value of the NFT is typically linked to the perceived value of the artist's work. In other words, the artist's reputation gives the NFT value, not any "network effect" or promotion by an identifiable third party. The fortunes of the purchasers of art NFTs typically are not linked to each other, or to the success of the promoter's efforts, because the value of the NFT emanates instead from the art with which it is associated.

However, this analysis is highly dependent on facts and circumstances. For instance, if a creator launches a collection of NFTs with similar characteristics, where the value of the NFTs within the collection likely rise and fall together, the SEC or a court could find that a common enterprise exists.

Further, it is unclear whether an entity created by smart contract (for example, a decentralized autonomous organization or DAO) might constitute a common enterprise, and any associated NFT issued in the collection viewed as an equity-like security. The decentralization of networks can impact the common enterprise analysis. Because a true decentralized environment is member-owned without centralized leadership, there is not a promoter, as needed for vertical commonality. While it is possible to view the collective members as having horizontal commonality, if no person possesses material nonpublic information, there is nothing to disclose and no party to make disclosures. It is important to note, however, that the use of a DAO does not, in and of itself, negate this prong. For further information on DAOs, see Practice Note, Decentralized Autonomous Organizations (DAOs): Overview.

For further information on this *Howey* prong, see Practice Note, Security Defined: Common Enterprise.

For further information on the application of *Howey* to crypto assets, see Practice Note, SEC Regulation of Digital Assets: SEC Approach to Digital Asset Regulation: Howey Test and FinHub Framework.

See also, Practice Note, Security Defined: Cryptocurrencies and Digital Assets.

Applying *Howey* Prongs to NFTs: Reasonable Expectation of Profits Based on the Efforts of Others

As applied to NFTs, analysis of this prong, sometimes subdivided into two separate prongs, focuses on the:

- Use of the proceeds from sale of the NFTs.
- Rights associated with the NFTs.
- Manner in which the NFTs are minted, distributed, and sold.
- How the NFTs are marketed.

Applying *Howey* Prongs to NFTs: Reasonable Expectation of Profits

As applied to NFTs, critical to the analysis is whether the purchaser expects the value of the NFT to increase due to:

- Capital appreciation resulting from the development of the NFT/NFT-related network or receipt of earnings from the use of the funds from the sale of the NFT; or
- Purely market-based forces that impact the supply and demand of the NFT (like the value of gold and silver).

Capital appreciation and participation in earnings are more likely to be viewed as profit for purposes of this prong, whereas value increases based on market forces are less likely to be viewed as profit. Where the NFT is marketed such that investors are lured by a promoter or other third party with the promise of profit, this prong is likely to be met.

In the case of art NFTs, investors are often lured not by profit but by interest in the NFT media itself. While purchasers are generally aware that their purchase may appreciate in value, typically it is not as a result of the initial investment. The art NFT media is already developed by the time it is purchased and any increase in value is generally based on market forces. Additionally, art NFTs generally do not offer profits in the form of dividends. If dividends or royalties are a characteristic of the NFT, then the NFT may draw increased scrutiny under the expectation-of-profits analysis.

NFT collectibles may require a more rigorous facts-and-circumstances analysis as to whether there is an expectation of profits. Numerous factors in the SEC framework may weigh in favor of the SEC finding this prong met for NFT collectibles, , especially if the NFTs carry the following characteristics:

- They trade in a secondary marketplace.
- Purchasers may be viewed as relying on the expertise of the AP to grow the value of the asset and network.
- They are marketed, directly or indirectly, using the expertise of the AP to grow the value of the digital asset.
- They use terms indicating the purchase is an investment.
- The asset is promoted as a way to develop the network or asset or is accompanied by an implied or explicit

promise to build the business (as opposed to delivering currently available goods).

For further information on this *Howey* prong, see Practice Note, Security Defined: Expectation of Profits.

For further information on the application of *Howey* to crypto assets, see Practice Note, SEC Regulation of Digital Assets: SEC Approach to Digital Asset Regulation: Howey Test and FinHub Framework.

See also, Practice Note, Security Defined: Cryptocurrencies and Digital Assets.

Applying *Howey* Prongs to NFTs: Profits Based on the Efforts of Others

As applied to NFTs, this element is met if a purchaser reasonably expects to rely on the efforts of an AP and those efforts are undeniably significant, essential managerial efforts which affect the failure or success of the enterprise, as opposed to efforts that are more ministerial in nature. If the NFT is already built and the funds are not being used to build a business operation, then those factors would weigh against the SEC concluding that the NFT is a security.

For further information on this *Howey* prong, see Practice Note, Security Defined: From the Efforts of Others.

For further information on the application of *Howey* to crypto assets, see Practice Note, SEC Regulation of Digital Assets: SEC Approach to Digital Asset Regulation: Howey Test and FinHub Framework.

See also, Practice Note, Security Defined: Cryptocurrencies and Digital Assets.

Application of *Ripple Labs* Ruling to NFTs

In addition to the *Howey* prongs discussed above, a crypto-asset securities analysis under US law can no longer be undertaken without consideration of the ruling in *Securities and Exchange Commission v. Ripple Labs, Inc., et al.*, a case brought by the SEC against payment settlement system and currency exchange network Ripple Labs, Inc. and its senior leaders (collectively, Ripple) for conducting an unregistered offer and sale of crypto-asset securities in connection with issuance by Ripple of the XRP token, a well-known cryptocurrency (1:20-cv-10832 (S.D.N.Y. 2020)). On July 13, 2023, Judge Analisa Torres of the SDNY issued an order granting in part and denying in part cross motions for summary judgment filed by Ripple and the SEC, holding that, under the *Howey* test:

- Programmatic sales (through the use of trading algorithms) of XRP to retail investors on digital asset exchanges did not constitute the offer and sale of securities because:
  - these sales were blind bid/ask transactions; and
  - retail buyers could not have known if their payments of money went to Ripple or another seller of XRP.
- Institutional sales of XRP did constitute the offer and sale of securities because:
  - institutional investors would have purchased XRP with the expectation that they would derive profits from Ripple's efforts; and
  - Ripple led institutional investors to believe Ripple would use the capital received from its institutional sales to improve the market for XRP and develop uses for the XRP ledger, thereby increasing the value of XRP.
- Other distributions did not constitute the offer and sale of investment contracts because recipients of the other distributions did not pay money or "some tangible and definable consideration" to Ripple for their XRP.

This important distinction between *types* of crypto-asset sales has application in the NFT context, though may not necessarily be determinative of whether or not a particular NFT is a security. Nevertheless, *Ripple* must be considered in any NFT offer-and-sale crypto-asset security analysis. For further detail, see Legal Update, SEC v. Ripple Labs: SDNY Holds Unregistered Sales of XRP Token Directly to Institutional Investors Violated US Securities Laws but Retail XRP Sales on Public Crypto Exchanges Did Not. But see Legal Update, SEC v. Terraform Labs: SDNY Judge Denies Motion to Dismiss, Declines to Follow Ripple Labs Ruling.

First SEC NFT Crypto-Asset Securities Enforcement Actions

Though respondents in these matters neither admitted nor denied the charges and no legal proceedings were conducted, the SEC's first NFT crypto-asset securities cases provide some insight into the SEC's view on application of the *Howey* analysis to NFTs.

SEC Impact Theory Crypto-Asset Securities NFT Action

On August 28, 2023, the SEC issued a cease-and-desist order settling charges against Impact Theory, LLC, a media and entertainment company, for the unregistered offering of certain NFTs the SEC found to be crypto-asset securities. This marks the SEC's first NFT crypto-asset securities enforcement action. The order states that

Impact offered and sold NFTs known as Founder's Keys, raising approximately $29.9 million in ether (ETH) from hundreds of investors, including investors across the US.

According to the order, Impact violated Sections 5(a) and 5(c) of the Securities Act by offering and selling securities without having a registration statement filed or in effect with the SEC or qualifying for an exemption from SEC registration. Founder's Keys were offered and sold as investment contracts and therefore as securities under the *Howey* test.

According to the order, the Founder's Keys purchasers had a reasonable expectation of obtaining a future profit based on Impact's managerial and entrepreneurial efforts with respect to the NFTs. For example, prior to the Founder's Keys offering, Impact invited investors to view the purchase of a Founder's Key as an investment in Impact's business, stating that investors would profit from their purchases if Impact was successful in its efforts. Among other things, Impact emphasized that:

- It was "trying to build the next Disney."
- If successful, it would deliver "tremendous value" to Founder's Keys purchasers.
- The future value of the Founder's Keys would be significantly greater than their purchase price.
- The value of Founders Keys would be derived from the company's efforts.
- Impact's view was that the fortunes of Founder's Key purchasers, Impact as a business, and Impact's founders were all interconnected.

According to the order, Impact made numerous statements that resulted in prospective and actual purchasers of Founder's Key NFTs, stating on an Impact online platform that they viewed Founder's Keys as investments into the company and understood Impact's statements to mean that the company's development of its projects could translate to appreciation in value of the Founder's Keys over time.

The order further states that Impact also traded the Founder's Keys on various secondary market crypto-asset trading platforms, and Impact stated on its website and social media channels that Founder's Keys could be purchased and sold on two secondary market platforms. Impact also programmed the smart contract for the Founder's Keys traded on secondary market platforms so that Impact received a 10% royalty on each secondary market sale, which generated approximately $978,000 worth of ether in royalties for Impact.

According to the order, Impact did not admit or deny the findings of the SEC but consented to the entry of the order to settle the proceedings. The settlement requires Impact to, among other things:

- Cease and desist from committing or causing any violations or any future violations of Sections 5(a) and 5(c) of the Securities Act.
- Pay a combined total of more than $6.1 million in disgorgement, prejudgment interest, and a civil penalty.
- Return monies that injured investors paid to purchase Founder's Keys.
- Destroy all Founder's Keys in its possession or control.
- Publish notice of the order on its websites and social media channels.
- Eliminate any royalty that Impact might otherwise receive from future secondary market transactions involving the Founder's Keys.

SEC Commissioners Hester M. Peirce and Mark T. Uyeda issued a dissenting statement, noting that the typical cure for a registration violation is a rescission offer and that the order and settlement raise difficult questions regarding NFTs and the US securities laws.

SEC Stoner Cats Crypto-Asset Securities NFT Action

Shortly after Impact Theory, on September 13, 2023, the SEC issued a cease-and-desist order settling charges against Stoner Cats 2, LLC (SC2) for conducting an unregistered offering of NFTs. On July 27, 2021, SC2 offered and sold to the public 10,320 NFTs and generated gross proceeds in ether (ETH) equal to approximately $8.2 million, which was used to fund the production of an animated web series, Stoner Cats.

The SEC claims that SC2 violated Section 5(a) and 5(c) of the Securities Act by offering and selling securities by means of interstate commerce without having a registration statement filed or in effect with the SEC or qualifying for an exemption from SEC registration. The SEC states that SC2 offered and sold the NFTs as investment contracts, and therefore securities, under the *Howey* test.

According to the SEC, SC2 had a high-profile marketing campaign, which promoted the NFTs and highlighted benefits of owning the NFTs, including:

Exclusive access to Stoner Cats content, as well as access to other content that the Stoner Cats producers created in perpetuity.

Exclusive access to the Stoner Cats community, including events, contests, and opportunities to engage with the creators of the animated show.

The option for holders to resell the NFTs on the secondary market.

Additionally, the NFTs were configured so that SC2 received a 2.5% royalty for each transaction in the NFTs on a certain secondary market platform, which created an incentive for SC2 to encourage individuals to buy and sell the NFTs on the secondary market. SC2 marketing led investors to reasonably expect to profit based on SC2's managerial and entrepreneurial efforts.

Without admitting or denying the SEC allegations, SC2 agreed to:

Destroy all remaining Stoner Cats NFTs in its possession, custody, or control.

Publish notice of the order on SC2s website and social media.

Cease and desist from committing or causing any violations of Sections 5(a) and (c) of the Securities Act.

Pay a civil money penalty of $1,000,000 to the SEC.

SEC Commissioners Hester M. Peirce and Mark T. Uyeda issued a dissenting statement, noting that the mere fact that money was involved does not transform NFTs into securities. The dissent argues that the application of securities laws does not make sense in this case and instead the SEC should "lay out clear guidelines for artists and other creators who want to experiment with NFTs as a way to support their creative efforts and build fan communities."

Are NBA Top Shot NFTs Securities?

The above analysis is likely being undertaken in a case that may be largely determinative of many of these open questions for NFTs going forward. On May 12, 2021, a class action complaint was filed against Dapper Labs, developer of the NBA Top Shot NFTs, and its CEO, alleging that the NFTs offered and sold on the platform were unregistered securities. Among other things, the complaint alleges that Dapper Labs "used their control over the platform to prevent investors from cashing out" their NFT purchases. The case was removed to federal court by Dapper Labs and on December 27, 2021, plaintiff class filed an amended complaint.

The amended complaint alleges that Top Shot "Moments" NFTs "derive their value from the success or failure" of defendants and therefore qualify as investment contracts under the *Howey* framework. Plaintiffs assert that Moments NFTs satisfy the first *Howey* prong (investment of money) and that the second prong (common enterprise) is satisfied because the investors are passive participants in the Top Shot enterprise, which is centrally controlled and managed by defendants and reliant on the underlying Flow blockchain, which was also developed by defendants. Importantly, the amended complaint argues that purchasers obtained Moments NFTs reasonably expecting profits, in part due to the fact that NFTs have the potential to greatly increase in value and that these purchasers expected these profits to be derived from the managerial efforts of defendants.

On February 22, 2023, the SDNY denied defendants' motion to dismiss plaintiffs' amended complaint under Rule 12(b)(6) of the Federal Rules of Civil Procedure, holding that plaintiffs adequately pled that NBA Top Shot Moments NFTs were investment contracts that constituted securities under the *Howey* test (*Friel v. Dapper Labs, Inc.*, 2023 WL 2162747 (S.D.N.Y. 2023)).

For further information, see Legal Update, SDNY Allows Lawsuit Alleging NBA Top Shot NFTs Are Securities to Proceed.

OpenSea Insider Trading Case

Although the SEC is not involved in the action, on May 3, 2023, a SDNY jury found Nathaniel Chastain, a former manager at OpenSea, guilty of wire fraud and money laundering in connection with his purchase and later sale of NFTs featured on the OpenSea website. This was the first conviction obtained in an insider trading case involving digital assets on a crypto-asset platform (see Legal Update, Federal Prosecutors Secure First Ever Crypto Insider Trading Conviction in OpenSea NFT Case). As this case was brought under traditional fraud statutes and not as securities fraud, the DOJ was not required to prove the NFTs at issue were securities in this case.

Other Elements of NFTs that May Trigger Application of Securities Laws

Application of Securities Laws to Art or Collectibles

Typically, unless packaged as part of a profit-making scheme, individual sales of artwork or collectibles do not trigger the securities laws, and even when part of a profit-making scheme there still must be a common enterprise.

NFTs that are marketed and sold as digital art are unlikely to trigger the securities laws, except where:

- A third party seeks to use funds raised in NFT sales to fund a business; or
- Purchasers buy NFTs based on representations of appreciation potential.

For example, if an NFT issuer or promoter uses certain marketing practices, such as encouraging (or even requiring) purchasers to further promote NFT sales, this could be viewed by the SEC as supporting a finding of a common enterprise because the purchasers as a group may appear to have little control over the venture and depend on the promoter's marketing efforts, as well as each other's efforts, to ensure the NFTs have resale value on secondary markets.

Where purchasers are prompted to promote NFTs via their networks, if the efforts of the promoter (as opposed to purchasers) are the undeniably significant ones – "those essential managerial efforts which affect the failure or success of the enterprise" – then investors might be found to have reasonably expected profits as the result of reliance on the managerial efforts of others under *Howey*.

Fractionalized NFTs (F-NFTs)

Fractionalized NFTs (F-NFTs) divide ownership of an NFT into fractions, providing individual ownership of pieces of the NFT so that multiple individuals (typically hundreds or thousands) can partake in the benefits of the underlying asset. In this model, a finite number of fungible tokens represent equal fractions of a divisible whole, with no one token representing any one part of an NFT, giving all purchasers of the token identical exposure to the underlying asset. This creates a pool of liquidity centered around one specific NFT or a group of NFTs. In this scenario, a central party:

- Acts as the issuer of the fractionalized fungible representation of the NFT.
- Uses the capital to operate or launch the business.
- Manages the underlying NFT asset or assets.

In some circumstances, the SEC has found fractionalized interests to be securities, even where the underlying assets were not necessarily securities. For example, the SEC has concluded that fractional, tenant-in-common interests in event spaces (property) were securities, fractional undivided oil-and-gas interests were securities, and fractional ownership interest in wells and oilfields were securities.

Fractionalized art sales using blockchain technology, which divide artwork into digital shares and sell them to investors, appears to be gaining in popularity. With such a product, it appears likely that the first and second prongs of *Howey* are met, but the third prong – whether there is an expectation of profits based on the efforts of others – may be difficult to prove because the motivation for purchasing artwork may be personal rather than for economic gain. Therefore, platforms offering fractionalized art sales that advertise them as investments or for economic gain are more likely to attract regulatory scrutiny.

It is noteworthy that SEC Commissioner Hester Peirce has reportedly remarked that "the whole concept of an NFT is supposed to be non-fungible, [therefore] in general, it's less likely to be a security," but if issuers decide to "sell fractional interests" in NFTs, "you better be careful that you're not creating something that's an investment product, that is a security."

Perpetual Royalties

Automated royalty payments, which can be programmed into an NFT's smart contract, have the potential to allow NFT creators to monetize their work in perpetuity and provide the creator a percentage of each resale. For example, in an initial sale, Beeple sold his NFT Crossroads for $67,000. Thereafter, he earned ten percent on resale of the work as a result of the perpetual royalty triggered on resale, earning him a greater profit than he received from the original sale.

By comparison, in the traditional art world, artists typically do not receive resale percentages. In the case of one artist receiving perpetual royalties, even if a sales platform receives a commission, it is not likely to meet the definition of a security. NFTs can also be structured to pay a perpetual royalty fee to certain stakeholders (artists, creators, initial purchasers) each time the NFT is sold in the future. In the case of F-NFTs, all such holders could receive a royalty payment any time the underlying NFT is sold.

When more than one person is receiving a royalty payment, such as the case with perpetual royalties – and especially royalties on F-NFTs – these arrangements can resemble dividends or interest on a debt security. These type of arrangements warrant more scrutiny in determining whether there is a common enterprise and an expectation of profits based on the efforts of others.

For example, when the issuer is entitled to a royalty in perpetuity, there can be vertical commonality in some circumstances if the success of the creator (typically

playing the role of promoter) is linked to the buying public. If perpetual royalties are made available to NFT holders (purchasers downstream from the creator), this could create horizontal commonality as well. In addition, in circumstances in which NFT issuers/promoters grant royalty rights to purchasers via the NFT's underlying smart contract, this may warrant additional scrutiny as to whether a purchaser had a reasonable expectation of profits. If it appears to be akin to interest or a dividend, it is more likely to be the type of revenue-sharing agreement that satisfies *Howey*'s third prong. An asset is also more likely to be a security when a royalty-bearing NFT is fractionalized and pooled with other revenue-generating assets.

NFT Trading Platforms May Be Exchanges Subject to SEC Rules

Platforms that offer trading of digital assets that are securities (sometimes referred to as crypto-asset securities) and that operate as exchanges as defined by the federal securities laws must register with the SEC as a national securities exchange or be exempt from registration, and may also be required to register as a broker-dealer and/or or clearing agency as well. Failure to register risks enforcement actions by the SEC or class action lawsuits by disgruntled purchasers. NFT trading platforms or any platform that offers an NFT for sale must be aware of these obligations.

In addition, the SEC has proposed to expand the definition of the term "exchange" under the Exchange Act, which would capture many crypto-asset trading platforms, potentially including certain NFT marketplaces (see Practice Note, SEC Regulation of Digital Assets: Proposed Proposed Amendments to "Exchange" Definition).

NFT SEC Compliance: Recommendations and Best Practices

While it remains debatable whether the securities laws apply to NFT trading platforms, it seems clear that these platforms will continue to grapple with some of the same issues as securities exchanges and other digital asset exchanges. Therefore platforms, including NFT exchanges (both centralized and decentralized) must remain aware of the full scope of obligations that accompany the offer and sale of securities and consider implementing safeguards to reduce the risk of liability for non-compliance and unlawful activities, such as insider trading.

To mitigate SEC scrutiny of an NFT venture, NFT market participants should consider the following:

- **Limit NFT rights.** The lowest risk NFTs from an SEC (and CFTC) compliance perspective are those NFTs that do not confer any rights to the holder other than:
  - the right to access the NFT media;
  - the right to transfer the NFT to a third party; and
  - the right to receive a physical consumptive item of nominal value.
- **Avoid promotional activities.** NFT sellers, creators, and their agents, vendors or other affiliated third parties should not design, sell, market, or promote NFTs:
  - as an opportunity for investment or profit;
  - to drive price appreciation; or
  - for price appreciation based on future efforts of the creator or other third party.
- **Do not fractionalize.** Fractionalization of an NFT typically results in the issuance of fungible tokens to purchasers, and therefore may be more likely to be viewed as securities under current SEC guidance if the success or failure of the venture, and the purchasers rely on the efforts of the fungible fractionalized token issuer.
- **Limit royalties to the artist.** While perpetual royalties ostensibly can be paid to all or some NFT purchasers, doing so could result in the expectation of profits based on the efforts of the artist, whereas perpetual royalties paid only to the creator are unlikely to raise such a presumption as purchasers would receive no downstream benefit.

Tax Treatment of NFTs

IRS Guidance on Taxation of NFTs

On March 21, 2023, the IRS published its first guidance on the taxation of NFTs in Notice 2023-27, in which it announced its intention to issue guidance treating certain NFTs as collectibles for retirement plans under IRC Section 408(m). The acquisition of a collectible by an IRA or an individually directed account in a retirement plan is therefore treated as a distribution from the retirement account in an amount equal to the cost of the collectible. The constructive distribution is taxable, making collectibles generally unsuitable investments for retirement plans.

The IRS has not previously addressed NFTs in any of its limited cryptocurrency guidance, including Notice 2014-21,

which treats convertible cryptocurrency as property for tax purposes, and not as cash or currency.

The term "collectible" currently includes any:

- Work of art.
- Rug or antique.
- Metal or gem.
- Stamp or coin.
- Alcoholic beverage.
- Other tangible personal property specified by the Secretary of the Treasury.

(IRC § 408(m)(2).)

Certain coins and bullion are excluded from the definition of collectibles (IRC §408(m)(3)).

Treating an NFT as a collectible also has relevance for other US federal income tax purposes, including the long-term capital gain rate. The maximum long-term capital gains rate for collectibles is 28 percent.

Pending the release of future guidance, the IRS intends to determine whether an NFT is a Section 408(m) collectible by analyzing whether the NFT's associated right or asset is a Section 408(m) collectible under a look-through analysis. For example, an NFT that certifies ownership of a gem is a collectible while an NFT that provides a right to use or develop a plot of land in a virtual environment is not a collectible. Some states have already implemented this look-through approach for sales tax purposes.

It is unclear whether the look-through analysis in Notice 2023-27 will apply only to determine whether an NFT is treated as a collectible or more broadly.

Purchasing NFTs with Cryptocurrency

An initial point of consideration for the taxation of an NFT is whether it was purchased with a cryptocurrency. An acquisition of an NFT using cryptocurrency results in taxable transactions for both the buyer and the seller. This is because the NFT buyer is buying property (the NFT) with other property (cryptocurrency). The buyer's gain is taxable if the fair market value of the cryptocurrency used to buy the NFT is greater than the buyer's tax basis in the cryptocurrency.

If, on the other hand, the NFT is sold for cash, the seller has a taxable transaction but the buyer does not. The amount of taxable gain or loss for the seller is the difference between its adjusted tax basis in the NFT and the amount received for the NFT.

Taxation of Sale or Exchange of an NFT

Just as with other types of property, the tax treatment of a sale or exchange of an NFT depends on whether the NFT is a capital or noncapital asset. Gain or loss on an NFT transaction is treated as capital or ordinary, depending on whether the taxpayer is an investor or trader (capital) or a dealer or creator (ordinary). Whether the holder of an NFT is an investor, trader, dealer, or creator is a mixed question of fact and law.

Taxation of NFT Investors and Traders

An investor is typically a taxpayer profiting solely from price fluctuations and income earned on the investments they hold. Investors are not engaged in a trade or business so expenses attributable to their investments and losses arising from their investments may not be deductible for tax purposes.

Traders are professional investors that are considered to be engaged in a trade or business for tax purposes. Traders buy and sell capital assets to profit from favorable changes in market prices. Neither the Internal Revenue Code nor the Treasury regulations define the term "trader," and the court cases addressing traders turn on the frequency, extent, and regularity of the trading activity, the taxpayer's investment intent, and the nature of the income derived from the activity. A trader is engaged in a trade or business so ordinary and necessary expenses attributable to their investments may be deductible for tax purposes.

For an individual investor or trader, the holding period of the NFT determines whether:

- A preferential long-term capital gain rate applies (a maximum rate of 20 percent, with a 28 percent rate applicable to NFTs that are treated as collectibles); or
- A short-term capital gain rate applies (taxed at ordinary income tax rates, with a current top rate of 37 percent for individuals).

In general, the sale of an NFT that is held for more than 12 months should result in a long-term capital gain or loss, while an NFT held for less than 12 months should result in a short-term capital gain or loss. A capital loss is subject to special limitation rules that apply to capital assets, which may result in a capital loss being non-deductible.

Taxation of NFT Dealers

Dealers are distinguishable from investors and traders. A dealer earns income from a markup on items sold from

their inventory, or stock-in-trade, to customers in the ordinary course of the dealer's trade or business. A dealer often makes markets by quoting the bid and ask prices at which they are willing to buy and sell an item. The courts and the IRS have found a combination of factors to be determinative of dealer status, including:

- Having a large volume of sales and purchases.
- Holding oneself out to the public as a dealer.
- Selling items out of inventory to customers.
- Profiting from commissions rather than from appreciation in the value of an item.

Infrequent and isolated transactions do not qualify as dealer transactions. Dealers earn ordinary income and loss on the transactions that are part of their trade or business activities and are accordingly subject to tax on their income at graduated rates (with a current top rate of 37 percent for individuals). A dealer may deduct ordinary and necessary business expenses.

Taxation of NFT Creators

A creator is commonly understood to be the artist that created an NFT and offers it for sale in the marketplaces. A creator of NFTs that is engaged in a trade or business of creating NFTs recognizes ordinary income or loss on the disposition of an NFT and may additionally be subject to self-employment tax on any income earned on the disposition. A creator of NFTs that is engaged in a trade or business of creating NFTs may also deduct ordinary and necessary business expenses.

NFT Broker Reporting Requirements

Under the rules of IRC Section 6045, brokers must file information returns (on IRS Form 1099-B) showing the names and addresses of their customers and the gross proceeds of transactions effected through the broker and to furnish their customers with information statements. Prior to 2022, there was no guidance on tax and information reporting for NFTs. Nevertheless, an exchange or platform for NFTs was still required to consider whether they were a broker required to file information returns (including IRS Forms 1099 and 1099-B) showing the name and address of the account holder and details regarding any sales.

The Infrastructure Investment and Jobs Act of 2021 expanded the definition of "broker" under information reporting rules to include "any person who (for consideration) is responsible for regularly providing any service effectuating transfers of digital assets on behalf of another person" (IRC § 6045(c)(1)(D)). This expanded definition is effective for returns required to be filed, and statements required to be furnished, after December 31, 2023. Although the change to the definition of broker would have originally required broker information reporting for digital assets beginning in 2024, the IRS has delayed implementation of the reporting rules until final regulations are issued (IRS Announcement 2023-2).

A digital asset is defined as "any digital representation of value which is recorded on a cryptographically secured distributed ledger or any similar technology as specified by [the IRS]" It is unclear whether NFTs are digital assets for this purpose, although the instructions to IRS Form 1040 indicate that NFTs are digital assets for purposes of answering the question on that form relating to whether the taxpayer has received, sold, exchanged, or otherwise disposed of a digital asset during the taxable year.

*BakerHostetler Contributing Authors: *Robert A. Musiala Jr. (lead author/editor), Joanna Wasick, Teresa Goody Guillen, Jonno Forman, Keith Murphy, Adam Gale, Nick Mowbray, Linda Goldstein, Amy Mudge, Janine Bowen, George Stamboulidis, Lauren Bass, Veronica Reynolds, Erika Vela, Christina Gotsis.*