# The Banking Law Journal

Established 1889

**An A.S. Pratt™ PUBLICATION** **MARCH 2023**





LexisNexis

# THE BANKING LAW JOURNAL

**VOLUME 140** **NUMBER 3** **March 2023**



LexisNexis®

**QUESTIONS ABOUT THIS PUBLICATION?**

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please call:
Matthew T. Burke at ..... (800) 252-9257
Email: ..... matthew.t.burke@lexisnexis.com
Outside the United States and Canada, please call . . . . . (973) 820-2000

For assistance with replacement pages, shipments, billing or other customer service matters, please call:
Customer Services Department at . . . . . (800) 833-9844
Outside the United States and Canada, please call . . . . . (518) 487-3385
Fax Number . . . . . (800) 828-8341
Customer Service Website . . . . . http://www.lexisnexis.com/custserv/

For information on other Matthew Bender publications, please call
Your account manager or . . . . . (800) 223-1940
Outside the United States and Canada, please call . . . . . (937) 247-0293

ISBN: 978-0-7698-7878-2 (print)
ISSN: 0005-5506 (Print)

Cite this publication as:

The Banking Law Journal (LexisNexis A.S. Pratt)

Because the section you are citing may be revised in a later release, you may wish to photocopy or print out the section for convenient future reference.



Editorial Office
230 Park Ave., 7th Floor, New York, NY 10169 (800) 543-6862
www.lexisnexis.com

MATTHEW BENDER

(2023–Pub.4815)

# *Editor-in-Chief, Editor & Board of Editors*

THE BANKING LAW JOURNAL (ISBN 978-0-76987-878-2) (USPS 003-160) is published ten times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices.  For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquiries and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway, #18R, Floral Park, NY 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541. Material for publication is welcomed—articles, decisions, or other items of interest to bankers, officers of financial institutions, and their attorneys. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to THE BANKING LAW JOURNAL, LexisNexis Matthew Bender, 230 Park Ave, 7th Floor, New York, NY 10169.

POSTMASTER: Send address changes to THE BANKING LAW JOURNAL, A.S. Pratt & Sons, 805 Fifteenth Street, NW, Third Floor, Washington, DC 20005-2207.

# So, You Want to Start Accepting Crypto: Protecting Against Forfeiture Risks When Accepting Digital Assets

***By Martin J. Weinstein, Robert J. Meyer and Devin Charles Ringger****

*In this article, the authors analyze forfeiture risks associated with accepting cryptoassets and use historical examples to help companies weigh the risks and adopt compliance measures to mitigate the risk of forfeiture. In particular, the authors use the historical example of the Black Market Peso Exchange—a money laundering scheme used by Colombian drug cartels in the 1980s—as an example of the forfeiture risks faced by innocent owners of cryptoassets.*

As digital assets have become more popular and their usage more widespread (both in terms of total asset class value and in terms of the number of individual users),[1] companies ranging from automotive giants to neighborhood convenience stores have begun accepting (or thinking about accepting) digital assets as a method of payment for goods and services. There are many reasons why the prospect of accepting cryptoassets as a means of payment is appealing, but actually accepting such payments also carries risks. Chief among these is the possibility of civil forfeiture by federal and state governments if the assets used for payment had previously been obtained through illicit means.[2] In such circumstances, the acceptance of cryptoassets carries a risk of forfeiture, notwithstanding that the recipient is innocent of any of the underlying wrongdoing that subjected the payment to seizure in the first place.

This article analyzes forfeiture risks associated with accepting cryptoassets and uses historical examples to help companies weigh the risks and adopt compliance measures to mitigate the risk of forfeiture. In particular, this article uses the historical example of the Black Market Peso Exchange—a money laundering scheme used by Colombian drug cartels in the 1980s—as an example of the forfeiture risks faced by innocent owners of cryptoassets.

---

* Martin J. Weinstein is a partner in the Litigation Department and chair of Willkie Farr & Gallagher LLP's global Compliance, Investigations & Enforcement Practice Group. Robert J. Meyer is a partner in the firm's Litigation Department and a member of the firm's Compliance, Investigations & Enforcement Practice Group. Devin Charles Ringger is a senior associate at the firm in the Litigation Department and a member of the firm's Compliance, Investigations & Enforcement Practice Group. The authors may be contacted at mweinstein@willkie.com, rmeyer@willkie.com and dringger@willkie.com, respectively.

[1] The 2021 Crypto Crime Report, CHAINALYSIS (Feb. 16, 2021), https://go.chainalysis.com/2021-Crypto-Crime-Report.html.

[2] 18 U.S.C. § 981.

## CRYPTOASSETS AS A METHOD OF PAYMENT

Before a business decides to accept any form of digital asset as a method of payment, several important features of cryptoassets require analysis and discussion, as each plays an important part in informing the relevant legal analysis.

First, every type of cryptoasset is unique, each relying on its own set of underlying code, consensus mechanism, etc., and each reflecting a set of market participants that prefer to store their information on its blockchain. While this article uses certain examples based on particular blockchains, it is important to note that all blockchains are quite literally created unequally (as defined in their unique code and their unique protocol's feature set).

Furthermore, certain features of specific blockchains may pose different compliance risks that might lead prudent businesses to accept only certain cryptoassets, while eschewing others. For example, certain cryptoasset protocols make tracking transaction participants more difficult than other protocols because they maintain more stringent anonymizing characteristics;[3] this allocation of greater protections to buyer identities, in turn, makes compliance evaluations more difficult for potential sellers of goods and services, and may caution against their use in certain transactions.

Notwithstanding these distinctions, most major cryptoassets (and their underlying blockchain protocols) feature a core set of characteristics, each of which is relevant to the discussion of whether and how to accept cryptoassets as payment. These core features include:

- Regardless of their internal structure, cryptoassets are generally considered assets, and are not treated as monetary instruments under U.S. law;[4]
- Nearly all cryptoasset protocols are pseudonymous (identifying buyers and sellers solely using alphanumeric wallet addresses, which may or may not be attributable to a specific owner or owners); and
- Nearly all cryptoasset protocols record their transactions to a public and

---

[3] For example, Monero, which is even more anonymous than other blockchains, is currently the subject of a law enforcement "bounty" for assistance in deciphering its anonymity feature. This may give businesses pause from accepting payments denominated in Monero. See Kelly Phillips Erb, IRS Will Pay Up to $625,000 If You Can Crack Monero, Other Privacy Coins, FORBES, Sept. 14, 2020.

[4] See, e.g., Order Granting Defendant's Motion to Dismiss the Information, Florida v. Espinoza, No. F14-2923 (11th Jud. Cir. Miami-Dade Cnty. July 22, 2016).

transparent blockchain ledger that is publicly auditable, allowing for deep "on-chain" analysis of every market transaction throughout history, notwithstanding the fact that the pseudonymous nature of wallet ownership leaves the "last mile" of owner identification difficult, absent certain conditions (i.e., a subpoena issued to a centralized exchange (CEX) that may have been used to fund the cryptoasset wallet might be able to determine the identity of the wallet funder,[5] but if the wallet was instead funded using a decentralized exchange (DEX) that does not collect customer information, the funder's identity will not be ascertainable).

Taking each of these points in turn, monetary instruments are coins or currency of the United States (or of other countries), or one of several other categories of instruments strictly defined by the Secretary of the Treasury or by statute (e.g., traveler's checks, bearer negotiable instruments, bearer investment securities, checks, drafts, notes, money orders, etc.) that represent cash or a contract establishing a right or obligation to deliver or receive cash or another financial instrument.[6] These instruments are designed to stand in the place of fiat currency[7] (e.g., U.S. dollars) and generally have a fixed numerical value in a fiat currency that will not change even though the purchasing power of that fiat numerical value can potentially change (i.e., with inflation, etc.). Unlike fiat currency and other monetary instruments, cryptoassets are instead considered assets (like tangible goods) whose values in fiat currency denominations may be highly volatile because they are not backed or issued by a central government. This makes accepting cryptoassets in exchange for a good or service more akin to accepting a barter payment than accepting a fiat currency payment. And, most significantly, as will be explained below, as assets, cryptoassets may be the target of civil forfeiture laws even after they have been received for payment by

---

[5] For example, after a thief hacked into a crypto exchange recently and withdrew some $400 million in assets, one of the key pieces of forensic evidence left behind was the fact that the hacker needed to pay a transaction fee to transfer the stolen proceeds and had used his verified personal account at a CEX to send the necessary currency to cover the transaction fee. This indelibly connected the act of the theft to his personally identifying information previously collected by the CEX as part of its due diligence process and will likely play a key role in any ensuing investigation or prosecution. See Krisztian Sandor, FTX Hack or Inside Job? Blockchain Experts Examine Clues and a "Stupid Mistake," CoinDesk (Nov. 21, 2022), https://www.coindesk.com/business/2022/11/14/ftx-hack-or-inside-job-blockchain-experts-examine-clues-and-a-stupid-mistake/.

[6] See generally 31 U.S.C. § 5312(a)(3); 31 C.F.R. § 1010.100(dd).

[7] Fiat money or currency is a government-issued currency that is not backed by a physical commodity, but rather by the government that issued it. The value of fiat money is derived from the relationship between supply and demand and the stability of the issuing government.

an innocent third party, similar to how a stolen watch may be seized from a pawnshop after being purchased by the pawnshop owner from the thief.

The second key characteristic of cryptoassets is the pseudonymity of cryptoasset wallets, the method by which cryptoasset users store their cryptoassets. Although each holder of a cryptoasset must hold its cryptoassets in such a wallet (which is represented by an alphanumeric string of numbers and letters related to the user's unique cryptographic cipher, or "seed phrase," and is completely unique from all other wallets), crypto wallets are usually not directly attributable to any individual owner absent some inferential step requiring additional information not usually available to a potential counterparty.

Some wallet registrars require customers to provide identifying "Know Your Customer" (KYC) information that ties the wallet to the user, as would be required by a traditional bank.[8] Other wallet owners may be identifiable because they funded the wallet by buying the cryptoasset on a CEX that requires such identifying information and which could theoretically connect the wallet forever with the funding source, just like every transaction on the public blockchain forever publicly connects one participant with its previous counterparties. However, this wallet-funder information is not generally public, and would only be obtainable from a third party by using a subpoena.[9]

Furthermore, some hosts of digital wallets do not require the owner to present KYC information at all before opening the wallet. And some DEXs and similar services allow a wallet to be funded without even establishing a connection to a real person's identity or funding source. One service, Tornado.cash, allows an individual wallet holder to send or exchange value from

---

[8] Know Your Customer, or "KYC," information refers to the obligation that companies (and especially those dealing in financial services) know certain basic information about the counterparties with which or with whom they are doing business. Usually, KYC information includes information demonstrating the customer's identity (i.e., driver's license photos, passport photos, tax identification numbers, company incorporation documents, bank account information, etc.), the customer's eligibility to engage in the proposed business (i.e., proof of physical address or IP address confirmation to demonstrate the customer is located in an appropriate geography for location-specific eligibility or sanctions concerns, attestations affirming the customer's status as an eligible customer, etc.), and the risks involved in the business relationship (i.e., additional tax information, proof of a bank account in the customer's name, further attestations regarding the proper and improper uses of services rendered, etc.), and other similar characteristics. Some industries and companies are required to collect KYC information as a function of their operations, while others choose to collect KYC information to facilitate their compliance or risk-mitigation programs.

[9] See, e.g., Strobel v. Lesnick, No. 21-CV-01010-LB (N.D. Cal. Aug. 13, 2021) (Plaintiff was forced to subpoena digital wallet hosts to determine the owners of the wallets).

one wallet connected to a CEX with a wholly separate and disconnected wallet funded by the Tornado.cash DEX, in effect destroying the original traceability of the CEX wallet interaction and converting traceable cryptoassets into untraceable cryptoassets.[10] The use of such services allows users' identities to remain anonymous, even if the wallet remains unique to the user and public for all counterparties to see. As such, companies considering accepting cryptoassets must be aware that users can hide their identities from the company with very little ability for the company to prevent the user from doing so, and with very little opportunity to vet the ultimate source of the funding using the wallet address alone.

Moreover, insofar as a company can observe whether a wallet was funded by a DEX or a service such as Tornado.cash, the presence of such previous wallet interactions might be viewed as compliance red flags signaling that the assets contained within the wallet may have a dubious or illegal provenance. Given these characteristics, on August 8, 2022, the U.S. Department of the Treasury officially sanctioned Tornado.cash, which Treasury claims has been used to launder over $7 billion since its creation in 2019, and the original website is no longer accessible.[11] However, it is virtually certain that new websites providing similar services will emerge in the future, and companies should remain cognizant that DEX-funded wallets raise compliance red flags because of the difficulty associated with tracing the provenance of the wallets' funds.

Notwithstanding this pseudonymous characteristic that prevents ownership attribution, most cryptoasset transactions using blockchain technologies are publicly accessible and auditable by virtue of the public-facing nature of the blockchain, the entirety of which can usually be browsed in a simple web browser and can be downloaded for offline analysis as well. This allows any user to view a crypto wallet's entire contents, its full history of funding, and the history of all transactions associated with it.

## CRYPTOASSETS AS A MEDIUM OF ILLEGAL EXCHANGE

While proponents of cryptoassets laud these features for various reasons (the merits of which are beyond the scope of this article), the combined effect of these characteristics is the ability for wallet holders to remain anonymous while

---

[10] Tornado Cash, https://web.archive.org/web/20220804032605/ https://tornado.cash/ (static internet archive showing the contents of https://tornado.cash/ as of August 4, 2022). The original website, https://tornado.cash, is no longer accessible.

[11] Press Release, U.S. Dep't of the Treasury, U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash (Aug. 8, 2022), https://home.treasury.gov/news/press-releases/jy0916.

exchanging large sums of valuable assets nearly instantaneously. As such, cryptoassets (like cash) have emerged as an effective way to conduct illegal transactions while denying law enforcement the ability to effectively trace such transactions back to actual users who might face criminal penalties.

In 2019 alone, approximately $21.4 billion of various cryptoassets sent and received were traceable to illicit activities.[12] Although this accounted for just over 2% of all crypto transactions (a reflection of the growing size of the cryptoasset asset class as a whole), this volume of illegal activity is still a major concern, and as shall be explained, nearly all of this $21.4 billion could be subject to civil forfeiture even after it was used to purchase a bona fide good or service from an unwitting and innocent third party. This forms the basis of the legitimate concern that criminals could acquire significant amounts of cryptoassets illegally, such as through a ransomware attack or a fraud scheme, only to then launder them through the purchase of goods or services from a legitimate business that lacks the ability to determine the provenance and legal status of those funds with any degree of certainty.

Given the foregoing, even legitimate businesses that choose to receive payments in cryptoassets must know that the unique properties of cryptoassets make them very useful in achieving illegal or improper objectives. Whether serving as a financing mechanism for ransomware attacks, terrorism, human trafficking, or a means to escape the strictures of economic sanctions—as many commentators have recently noted in the context of the Russian aggression in Ukraine, the United States' imposition of strict economic sanctions, and the ease with which Russian wealth might nonetheless be transported abroad in violation of such sanctions—cryptoassets are quickly becoming a method of choice for transferring illegally obtained assets. The good news is that accepting cryptoassets as a form of payment does not, absent complicity, make a recipient criminally liable in such schemes; however, doing so does raise the specter that the cryptoassets thus obtained might later be subject to complex legal proceedings and potential seizure. And that is what this article is about—how you and your company may be unaware of previous criminality, but nonetheless remain subject to civil forfeiture unless you have taken the necessary steps to avoid it.

Fortunately, history does little better than repeat itself, and this problem—the unknown provenance of illegally acquired assets later used in legitimate transactions with innocent companies—has a strong historical antecedent in

---

[12] The 2021 Crypto Crime Report, supra note 1.

the Black Market Peso Exchange from the 1980s, which provides a useful pre-cryptoasset touchstone for similar transactions, as well as a good illustration of the current risks.

## THE BLACK MARKET PESO EXCHANGE

The Black Market Peso Exchange refers to a historic trade-based money laundering system devised to convert illegally obtained U.S. dollars into clean, fungible dollars that could then be put to the practical use of drug cartels. The process is relatively simple, and begins once the drug cartels export and sell illegal drugs within the United States, receiving U.S. dollars in exchange for their illegal drug sales. These dollars are not immediately useful in the cartels' home countries, and so the need arises to convert those criminal proceeds into their local currency. However, given the volume and source of the dollars generated by this criminality, the cartels needed to find an alternative to traditional methods of currency exchange, i.e., a black market.

Under this system, the cartels enter into a contract with local money traders in their home countries and sell their criminally obtained U.S. dollars in exchange for their local currency. The money traders take fees for this transaction, and the cartels walk away with local currency no longer directly connected to their criminal enterprises. Finally, the money trader then introduces the laundered U.S. dollars back into the U.S. banking system through a variety of methods to avoid detection. For example, money traders would frequently open fake bank accounts and deposit small amounts to avoid suspicion. At this stage of the process, the money traders have a large pool of U.S. dollars that they can use to purchase U.S. goods for local consumers in their home countries. Because taxes and tariffs in these countries are often very high for imported goods, consumers in Latin American countries would frequently use such money traders to import goods directly on their behalf (after purchasing them—perhaps unbeknownst to the local consumers—with criminal proceeds) in order to avoid paying the tariffs and taxes. In return, the money trader would again charge a fee for his or her services and purchase the goods on behalf of the consumers.

When first devised in the 1980s (and indeed, continuing to the present), the Black Market Peso Exchange posed two major problems for companies in the United States.

First, billions of dollars in drug money were being laundered by purchasing American goods and services. Manufacturers and retailers were unknowingly facilitating this money laundering scheme by selling their goods to the money traders.

Second, banks and other financial institutions were also unknowingly facilitating the money laundering scheme by hosting the money traders' financial accounts, which appeared legitimate to businesses selling goods or services.

## GOVERNMENT RESPONSE

Eventually, the U.S. government, financial institutions, and retail companies attempted to curtail this money laundering scheme. The United States initially passed regulations that required banks to report any transactions of more than $10,000.[13] However, this did not do enough to prevent the Black Market Peso Exchange from continuing to operate. Thus, in 1986, Congress passed the Money Laundering Control Act (MLCA), which made money laundering a federal crime.[14] It further prohibited individuals from knowingly engaging in financial transactions with proceeds that were generated from a set of crimes known as "specified unlawful activities."[15] The law requires "knowledge" on the part of third parties, but this knowledge element has been specifically defined to allow convictions of individuals or entities even if they do not know the particulars of the illegal activity.[16] Instead, it is sufficient that the recipient of ill-begotten funds/assets knows that the property came from some sort of criminal activity and that the property, in fact, constitutes the proceeds of a predicate offense. Knowledge may even be inferred from facts indicating that criminal activity is particularly likely, even if not certain.

Upon the passage of the MLCA, business and financial institutions also for the first time faced potential liability through civil forfeiture for facilitating money laundering activity. Often, these seizures targeted businesses set up for the purposes of money laundering or directly involved in the laundering of illicit funds; the first indictment of an offshore business engaged in the Black Market Peso Exchange, for instance, targeted a Panamanian jewelry business, Speed Joyeros S.A., which actively facilitated the laundering of drug proceeds through cash pick-ups, wire transfers, cashier's checks, and third-party bank checks, and whose principals conducted more than $100 million in business annually "knowing that the primarily Colombian-based customers were laundering millions of dollars in drug money from the United States through bulk

---

[13] Now codified under 31 U.S.C. §§ 5311 et seq. as part of the Bank Secrecy Act.

[14] 18 U.S.C. §§ 1956, 1957.

[15] Id.

[16] Id.

purchases of jewelry."[17] But even bona fide financial institutions fall within the MLCA's strictures and can face forfeiture actions if they fail to take the necessary precautions to avoid facilitating money laundering. For example, in 2007, American Express was required to pay $65 million to settle an enforcement action brought against the company for its failure to maintain an effective anti-money laundering program.[18]

In response to the MLCA and to address these risks, financial institutions began requiring customers to provide greater KYC information, so that they could reliably trace deposited funds back to the original owners. Businesses also began to require additional personal information for larger purchases, again employing stricter KYC rules to prevent purchases of goods and services using currency obtained through illegal activity. The government cracked down on companies "looking the other way" and continues to this day to bring large civil suits against companies that violate the statute. For example, in 2021, Sefira Capital LLC reached a settlement agreement with the Southern District of New York and the Drug Enforcement Agency, agreeing to forfeit $29 million to resolve the government's claims, representing approximately $22.5 million previously seized from Sefira and its subsidiaries, and an approximately $6.5 million payment in lieu of the forfeiture of certain real estate interests. As part of the settlement, Sefira agreed to conduct reasonable due diligence on future investors, and not to accept investment funds from any source other than the actual investor.[19]

## CIVIL FORFEITURE UNDER 18 U.S.C. § 981

The U.S. government's response to the Black Market Peso Exchange was also part of a larger movement to crack down on illegally obtained assets more generally, which led to renewed interest in civil forfeiture laws that would allow the government to seize ill-gotten assets. Historically, civil forfeiture in the United States was a holdover of English law and was used during the Prohibition era to seize bootleggers' property, but the resurgence of the War on Drugs in the 1980s led Congress to pass the Comprehensive Crime Control Act of 1984, which included as Title III the Comprehensive Forfeiture Act of 1984.

---

[17] Press Release, U.S. Attorney's Office for the Southern District of New York, More Than $40 Million Worth of Gold, Silver and Jewelry Forfeited in International Money Laundering Case (Apr. 12, 2010).

[18] Kevin Gale, AmEx Bank International to Pay $65M Penalty, S. Fla. Bus. J., Aug. 7, 2007.

[19] See Press Release, U.S. Attorney's Office for the Southern District of New York, Acting Manhattan U.S. Attorney Announces Settlement of Civil Forfeiture Claims Against Over $50 Million Laundered Through Black Market Peso Exchange (Jan. 12, 2021).

This act amended the Racketeer Influenced and Corrupt Organizations Act (RICO), while also clarifying what constitutes forfeitable property and creating a rebuttable presumption of forfeitability that allowed the government to seize first and defend the seizures in court later. These laws and their amendments are now codified in 18 U.S.C. § 981 and authorize the U.S. government to seize any property involved in a transaction that violates various sections of the U.S. Criminal Code, including, but not limited to: money laundering, illegal trafficking of controlled substances, stolen assets, fraud, and robbery.[20] In such circumstances (and where such property has been exchanged or transferred to a third-party company), prosecutors can bring a civil forfeiture action against the third party to recover the asset. This means that the government may seize an asset that has been transferred to a third party if that asset was originally the product of criminality, even if the new owner of the asset was not involved in the underlying criminality.

A civil forfeiture action may also be triggered by any conduct engaged in to evade U.S. economic sanctions, such as those imposed earlier this year against Russia in response to its military aggression against Ukraine.[21] Conduct used to evade economic sanctions has served as the basis of criminal prosecutions for violating the International Emergency Economic Powers Act (IEEPA), 50 U.S.C. §§ 1701–1705 (the act that underpins most U.S. economic sanctions imposed by the Treasury Department through its Office of Foreign Assets Control (OFAC)), and assets that were used to evade such sanctions have likewise been the subject of in rem proceedings directly against property on the grounds that it constituted "property involved in one or more money laundering offenses" under 18 U.S.C. §§ 1956 (money laundering) and/or 1957 (engaging in monetary transactions in property derived from specified unlawful activity), or was otherwise traceable to such property. Such "criminally derived property" under Section 1957 is forfeitable under 18 U.S.C. § 981, and its definition is broad enough to encompass large swaths of property involved in illegal activity.[22] The same could be true of other property involved in

---

[20] 18 U.S.C. § 981.

[21] Exec. Order No. 14,024, 86 Fed. Reg. 20,249 (Apr. 19, 2021).

[22] 18 U.S.C. § 1957(f)(2) ("the term 'criminally derived property' means any property constituting, or derived from, proceeds obtained from a criminal offense"); see also Charles Doyle, Money Laundering: An Overview of 18 U.S.C. § 1956 and Related Federal Criminal Law, CONG. RSCH. SERV., at 1 n.2 (Nov. 30, 2017), https://sgp.fas.org/crs/misc/RL33315.pdf (discussing various estimates of the number of § 1956 predicate offenses—the proceeds of each of which are also ported into § 1957 under 1957(f) as "specified unlawful activity"—and noting that even estimates of "250 or so" possible predicate offenses are "exceptionally conservative" given that 18 U.S.C. §§ 1956(c)(7)(A) and 1961(1)(A) also empower § 1957 forfeiture of

sanctions evasion, which could also be prosecutable on charges of conspiracy to violate IEEPA or to commit money laundering (18 U.S.C. § 1349), violation of the Bank Fraud Statute (18 U.S.C. § 1344), conspiracy to obstruct justice (if designed to obstruct a lawful investigation or government function) (18 U.S.C. §§ 371, 1505), making false statements to a financial institution (18 U.S.C. § 1014), various tax offenses, or other similar offenses. This is to say nothing of the myriad state civil forfeiture laws that could additionally be brought to bear on the asset holder, depending upon what jurisdiction the asset and the asset recipient are deemed to reside in.[23]

## THE INNOCENT OWNER DEFENSE TO CIVIL FORFEITURE

Fortunately, recognizing the forfeiture risks that 18 U.S.C. § 981 posed to truly innocent purchasers or recipients of forfeitable assets, Congress passed the Civil Asset Forfeiture Reform Act (CAFRA) in 2000, which created an "innocent owner defense" to civil forfeiture.[24] This defense allows a bona fide innocent owner to rebut the presumption of forfeitability, provided that the innocent purchaser can demonstrate that he or she exercised reasonable diligence before the purchase or receipt. Specifically, to avoid forfeiture, the current owner/company in possession bears the burden of proving that it was a "bona fide purchaser or seller for value (including a purchaser or seller of goods or services for value); and did not know and was reasonably without cause to believe that the property was subject to forfeiture."[25] However, the law makes clear that it is the claimant (i.e., the party seeking to be considered an

---

proceeds from state law felonies and § 1956(c)(7)(B) empowers forfeiture of proceeds from even foreign crimes and misconduct if the conduct at issue involves a financial transaction in the United States); Compl. for Forfeiture In Rem ¶ 4, United States v. Funds in the Amount of 73,293,750 AED (Approximately $20 Million) in the Possession & Control of Ras Al Khaimah Inv. Auth. (RAKIA), No. 3:20-cv-00126-JMK (D. Alaska June 3, 2020), ECF No. 1 (in rem action under § 981 against assets "involved in and traceable to [violations of the IEEPA] and a scheme to defraud financial institutions in the Republic of Korea").

[23] A full analysis of state-level forfeiture laws is beyond the scope of this article, but for more information on the legal forfeiture regimes on a state-by-state basis, see generally Dick M. Carpenter II et al., Policing for Profit: The Abuse of Civil Asset Forfeiture, Inst. for Just. (2d ed. Nov. 2015), https://ij.org/report/policing-for-profit-2/; id. App. B: Civil Forfeiture Law Citations and Other References, https://ij.org/report/policing-for-profit-2/appendix-b-civil-forfeiture-law-citations-and-other-references/; Steven Mark Levy, Federal Money Laundering Regulation: Banking, Corporate & Securities Compliance, § 28.04 (2d ed. Supp. June 2022) (state anti-money laundering enactments).

[24] 18 U.S.C. § 983(d).

[25] Id. § 983(d)(3)(A)(i)–(ii).

"innocent owner") who bears the burden of proving its innocence by a preponderance of the evidence.[26]

Furthermore, proving that a company was "reasonably without cause to believe that the property was subject to forfeiture" can be challenging.[27] Actual knowledge, for instance, may be proven by inference from circumstantial evidence suggesting that the assets were involved in previous criminality,[28] so a company will be imputed not just with knowledge in its actual possession but also with knowledge within its reasonable reach, as well. Thus, on top of being a highly fact-specific inquiry into the knowledge available to the company at the time of acquisition, the reasonableness of the company's conduct will additionally hinge on industry practices and the conduct of other, similarly situated companies and the precautions they are undertaking to ensure they are "reasonably without cause to believe." Likewise, it is not enough to show that a defendant was ignorant of forfeiture laws; an "innocent owner" must instead prove that it was ignorant of the fact that the property was involved in or traceable to a criminal violation.[29] However, the law is not as clear in other respects, and courts have also ruled that a claimant's mere awareness that the seller of an asset had engaged in fraudulent conduct did not, by itself, put the claimant on notice that every piece of the seller's property would be subject to forfeiture.[30]

In short, the grounds for civil forfeiture are many, various, and perilous to companies that choose not to ensure that they are "reasonably without cause to believe that the property [they are receiving is] subject to forfeiture."

## CIVIL FORFEITURE AND THE INNOCENT OWNER DEFENSE (AS APPLIED TO CRYPTOASSETS)

Fast-forward 40 years, and today there is now a risk that cryptoassets could be used to exchange ill-gotten criminal proceeds for "clean" assets/services/

---

[26] Id. § 983(d)(1).

[27] 36 Am. Jur. 2d Forfeitures and Penalties § 58 (2022); § 35:771. Innocent owner defense, 35 Fed. Proc., L. Ed. § 35:771 (2022); 25 Am. Jur. 2d Drugs and Controlled Substances § 234 (2022).

[28] United States v. One 1988 Checolet 410 Turbo Prop Aircraft, Dom. Rep. Registration Tail Number H1698CT, 282 F. Supp. 2d 1379 (S.D. Fla. 2003).

[29] United States v. An Int. in the Real Prop. Located at 2101 Lincoln Blvd., L.A., Cal., 729 F. Supp. 2d 1150, 1153 (C.D. Cal. 2010).

[30] United States v. Real Prop., Including All Improvements Thereon & Appurtenances Thereto, Located at 246 Main St., Dansville, Livingston Cnty., N.Y., 118 F. Supp. 3d 1310, 1330 (M.D. Fla. 2015).

monetary instruments in much the same way as the Black Market Peso Exchange was used previously. Instead of using laundered American dollars to purchase goods, bad actors can today use cryptoassets obtained through illicit activity to purchase goods and services as a method to effectively launder criminal proceeds. Furthermore, because cryptoassets are "assets" rather than "monetary instruments," businesses holding cryptoassets received as payment for their goods and services are subject to more expansive civil forfeiture laws than businesses holding monetary instruments.[31]

Today, recipients of cryptoassets may have those assets seized under the civil asset forfeiture statute, 18 U.S.C. § 981, if the assets in question constitute proceeds from (or are traceable to) a transaction or attempted transaction in violation of a very long list of criminal statutes: 18 U.S.C. §§ 1956, 1957, and 1960 (money laundering, specified unlawful activity, unlicensed money transmitting); 18 U.S.C. § 981(a)(1)(C) (describing offenses constituting "specified unlawful activity" or conspiracy to commit such offenses); 21 U.S.C. § 881 *et seq.* (property furnished or intended to be furnished in exchange for a controlled substance); or under the many provisions of 18 U.S.C. § 981(a)(1)(D)–(I) (describing large categories of crimes that could give rise to forfeitability). The same is true if cryptoassets in question constitute "criminally derived property" under 18 U.S.C. § 1957(f)(2) ("any property constituting, or derived from, proceeds obtained from a criminal offense").

Given these broad definitions, large swaths of cryptoassets traceable to criminal activity may be subject to seizure, even from subsequent purchasers who are ignorant of the assets' illegal provenance. Furthermore, the applicable statute of limitations provides two windows within which the government may file a civil forfeiture action: either within five years of discovering the alleged offense subjecting the property to forfeiture, or within two years of discovering that the property to be forfeited was involved in the offense, "whichever was later."[32]

---

[31] The forfeiture risks of holding cash and monetary instruments in "financial institutions in an interbank account," are markedly lower than holding assets, and are governed by 18 U.S.C. § 984 ("Civil forfeiture of fungible property"), provided that such cash and monetary instruments are not "traceable" to an offense giving rise to potential forfeiture. A full discussion of the "traceability" analysis conducted in evaluating the potential forfeiture of fungible assets is beyond the scope of this article.

[32] 19 U.S.C. § 1621; see also United States v. Kozeny, No. 05 CR 518 SAS (S.D.N.Y. Apr. 29, 2011) (Though it originally provided only for a five-year statute of limitations, the statute was amended in 2000 for the purpose of "enlarging the time in which the government may commence a civil forfeiture action. . . .") (quoting United States v. Twenty-Seven Parcels of Real Prop. Located in Sikeston, Scott Cnty., Mo., 236 F.3d 438, 440 (8th Cir. 2001)).

This gives the government years in which to investigate and discover the underlying crime giving rise to an asset's forfeitability prior to initiating a forfeiture action against the cryptoassets. Fortunately, and as described previously, an innocent recipient of cryptoassets subject to seizure may still defend against the seizure proceedings if it can successfully assert the "innocent owner defense" to civil forfeiture by showing by a preponderance of evidence that it is a "bona fide purchaser or seller for value (including a purchaser or seller of goods or services for value); and did not know and was reasonably without cause to believe that the property was subject to forfeiture."[33] Thus, if a company accepts cryptoassets that turn out to be traceable to illicit activity, those cryptoassets would be subject to forfeiture unless the recipient could prove that it was reasonably without cause to believe that the cryptoassets were obtained through illegal methods.

Further emphasizing this risk, the federal government is currently acting on President Biden's call for a whole-of-government approach to digital assets,[34] and numerous government departments have issued reports touching upon the seizure of cryptoassets, including by using criminal and civil forfeiture actions. For example, on September 16, 2022, the U.S. Department of the Treasury issued three such reports regarding the development of a coordinated interagency action plan for mitigating the illicit finance and the national security risks posed by digital assets, and outlining priorities to crack down on money laundering and countering the financing of terrorism using digital assets.[35]

That same day, the U.S. Department of Justice (the DOJ) issued a report of its own containing an entire Part III describing "initiatives that the Department and other law enforcement agencies have established to more effectively detect, investigate, prosecute, and otherwise disrupt crimes relating to digital assets, and to seize and forfeit those assets that constitute ill-gotten gains."[36] While this

---

[33] 18 U.S.C. § 983(d)(3)(A)(i)–(ii).

[34] See Exec. Order 14067, 87 Fed. Reg. 14143 (Mar. 14, 2022) ("Ensuring Responsible Development of Digital Assets").

[35] See Press Release, U.S. Dep't of the Treasury, Statement from Secretary of the Treasury Janet L. Yellen on the Release of Reports on Digital Assets (Sept. 16, 2022), https://home.treasury.gov/news/press-releases/jy0956; U.S. Dep't of the Treasury, The Future of Money and Payments Report Pursuant to Section 4(b) of Executive Order 14067 (Sept. 16, 2022), https://home.treasury.gov/system/files/136/Future-of-Money-and-Payments.pdf; U.S. Dep't of the Treasury, Crypto-Assets: Implications for Consumers, Investors, and Businesses (Sept. 16, 2022), https://home.treasury.gov/system/files/136/CryptoAsset_EO5.pdf; U.S. Dep't of the Treasury, Action Plan to Address Illicit Financing Risks of Digital Assets (Sept. 16, 2022), https://home.treasury.gov/system/files/136/Digital-Asset-Action-Plan.pdf.

[36] U.S. Dep't of Just., The Role Of Law Enforcement In Detecting, Investigating, And

section focuses on criminal forfeiture, which is not the subject of this article, it remains part of a broader call to crack down on illicit digital assets using forfeiture actions and builds upon the DOJ's prior use of civil forfeitures to achieve that goal.

For example, a previous DOJ report in June 2022 discussing how to strengthen international law enforcement of digital assets highlighted the strength of U.S. law allowing for civil forfeiture of digital assets: "[N]ot all foreign countries have asset-seizure authority outside of criminal prosecutions analogous to civil-forfeiture authorities under U.S. law—authorities that U.S. law enforcement agencies have regularly marshaled in the cryptocurrency sphere."[37]

Further emphasizing the point, the same day the DOJ issued the September 16, 2022 report, the DOJ simultaneously announced the establishment of the nationwide Digital Asset Coordinator (DAC) to address the "growing threat posed by the illicit use of digital assets to the American Public."[38] The press release particularly highlighted that, "[a]s members of the DAC network, prosecutors will learn about the application of existing authorities and laws to digital assets and best practices for investigating digital assets-related crimes, including for drafting search and seizure warrants, restraining orders, criminal and civil forfeiture actions, indictments, and other pleadings."[39]

These public statements and reports are not just aspirational; prosecutors are already seizing cryptoassets. The DOJ's 2021 Asset Forfeiture Policy Manual specifically explains its policies regarding the seizure of cryptoassets, and the DOJ has been active in bringing forfeiture actions.[40] For example, the DOJ has already sought forfeiture of hundreds of cryptoasset accounts and addresses used to launder hundreds of millions of dollars of cryptoassets traceable to exchange

---

Prosecuting Criminal Activity Related To Digital Assets (Sept. 6, 2022), https://web.archive.org/web/20221127185821/, https://www.justice.gov/ag/page/file/1535236/download.

[37] U.S. Dep't of Just., How To Strengthen International Law Enforcement Cooperation For Detecting, Investigating, And Prosecuting Criminal Activity Related To Digital Assets (June 6, 2022), https://www.justice.gov/media/1225896/dl?inline=.

[38] See Press Release, U.S. Dep't of Just., Justice Department Announces Report on Digital Assets and Launches Nationwide Network (Sept. 16 2022), https://www.justice.gov/opa/pr/justice-department-announces-report-digital-assets-and-launches-nationwide-network.

[39] Id.

[40] U.S. Dep't of Just., Asset Forfeiture Policy Manual (2021), https://www.justice.gov/criminal-afmls/file/839521/download (detailing the DOJ's cryptoasset seizure policies in Chapter 2(V)(B)).

hacks,[41] and by June 2021 had already executed 200 cryptoasset seizures.[42] And in February 2022, the DOJ announced its largest cryptoasset seizure in history when it seized 94,000 bitcoins (then valued at $3.6 billion) traceable to a 2016 computer hack of a cryptoasset exchange. While these bitcoins were not subject to civil forfeiture, but were instead seized directly from the thieves themselves, the seizure highlights the fact that prior to the seizure the thieves had almost eight years in which to spend their stolen bitcoins (which arguably remain subject to civil forfeiture to this day depending on when the underlying crimes were discovered). This proliferation of illegal assets throughout the market raises significant questions about the innocent recipients of those stolen and still-unseized bitcoins and whether they will be able to meet their burden to show that they are, in fact, "innocent owners." It also suggests that—while many of those recipients may successfully be able to claim that their bitcoins are not subject to seizure (because they could not have known about the illicit origins of the bitcoins at the time of their receipt from 2016 to 2022)—all companies going forward will have to pay closer attention than they did in previous years and will have to bring to bear the best contemporary industry practices for avoiding acquisition of valuable assets subject to seizure.

This is where things get tricky for a company wanting to accept cryptoassets because the transparency of blockchain transactions presents a double-edged sword of compliance opportunities and expectations.

On the one hand, the transparency allows proactive companies to thoroughly vet any potential transaction by performing detailed diligence on the history of the wallet associated with the purchase and the cryptoasset itself.

On the other hand, the fact that companies can conduct this kind of diligence suggests that it would be reasonable to conduct this diligence for relevant transactions. For example, a company accepting payment in cryptoassets might require that the cryptoasset wallets from which it receives

---

[41] United States v. 113 Virtual Currency Accounts, No. 20-606 (D.D.C. Mar. 2, 2020); Press Release, U.S. Dep't of Just., Two Chinese Nationals Charged with Laundering Over $100 Million in Cryptocurrency From Exchange Hack (Mar. 2, 2020), https://www.justice.gov/opa/pr/two-chinese-nationals-charged-laundering-over-100-million-cryptocurrency-exchange-hack; United States v. 280 Virtual Currency Accounts, No. 20-2396 (D.D.C. Aug. 27, 2020); Press Release, U.S. Dep't of Just., United States Files Complaint to Forfeit 280 Cryptocurrency Accounts Tied to Hacks of Two Exchanges by North Korean Actors (Aug. 27, 2020), https://www.justice.gov/opa/pr/united-states-files-complaint-forfeit-280-cryptocurrency-accounts-tied-hacks-two-exchanges.

[42] U.S. Dep't of Just., Office of the Inspector Gen., Audit of the United States Marshals Service's Management of Seized Cryptocurrency, at 2 (June 2022), https://oig.justice.gov/sites/default/files/reports/22-082.pdf.

funding be funded by CEXs (which can be subpoenaed for customer information, if later necessary), rather than by DEXs (which do not collect the requisite information and present a number of problems for civil subpoenas). Illustrating this example, Sotheby's Auction House, arguably the world's largest art auction house and a British-founded American multinational corporation headquartered in New York City, recently began accepting bids for expensive tangible and digital art denominated natively in the Ethereum cryptoasset, but only when potential bidders undertook extensive (and proactive) compliance steps prior to bidding. These steps include registering with a verified email address; submitting a government-issued ID and charging a $1.00 temporary hold to a credit card from a major credit card provider that corresponds to the same government-issued ID; funding the cryptoasset wallet used for bidding solely from a list of four verified CEXs; and submitting a "declaration statement providing Sotheby's with the billing address, along with supporting documentation for that billing address, before an invoice can be issued."[43] Sotheby's also reserved to itself the right to review all submitted information before releasing the invoice to the winning bidder, and collected taxes on all sales based upon the billing address of the buyer.

Most significantly, the vast majority of these requirements are not specifically imposed by law, but instead are proactively required by Sotheby's in an effort to ensure that—should problems arise at a later date regarding a sizable asset exchange involving cryptoassets—Sotheby's will have all of the most valuable pieces of KYC and compliance-related information necessary to demonstrate the reasonableness of its efforts and to identify both buyer and seller of its auctioned goods with specificity. Given the value of the assets at issue in Sotheby's high-end art auctions, these steps make perfect sense to ensure that Sotheby's will be able to show that it was reasonably without cause to believe that the cryptoassets it accepted were subject to forfeiture: for high-price purchases, the failure to perform due diligence carries the potential risk of civil forfeiture for cryptoassets carrying a significant value.

However, not all transactions would likely warrant or require this amount of effort and this amount of due diligence, even if they came with a risk of forfeiture. To be sure, this level of due diligence requires significant amounts of tedious work on the part of the company, whether by creating a department dedicated to performing crypto diligence in-house, or by engaging external support to achieve the same ends. Therefore, unlike the reasonable efforts

[43] See, e.g., Sotheby's, Bidder's Guide, NFTs and Currency at Sotheby's (June 10, 2021), https://www.sothebys.com/en/buy-sell/cryptocurrency-faq.

justified by large asset sales, performing due diligence for low-value transactions may not be warranted (from a cost perspective).

Simply put, the extent to which a company engages in proactive due diligence in order to manage its forfeiture risk is ultimately going to depend on a cost-benefit analysis in light of the specific asset values at issue and the risk of their forfeiture. The risk of having a cryptoasset seized simply may not justify expansive (and expensive) screening efforts if each transaction is sufficiently small (and absent some other indicia that the company's processes are being abused with such regularity or to such obvious illegal effect that the company's failure to implement a stronger compliance regime could create criminal fault).[44] But this is calculus well worth doing. And companies that fail to thoroughly vet cryptoasset transactions may not be able to take advantage of the innocent owner defense and may subsequently be vulnerable to civil forfeiture, even long after the transaction is completed, given the five-year statute of limitations on federal forfeiture actions.[45]

What form that due diligence process may take will depend on a number of factors. Sotheby's provides a good example on one end of the spectrum for companies involved in large-scale asset transfers. Such companies will certainly want to require customers to provide KYC information when making purchases with cryptoassets. They may also consider requiring the customer to sign a declaration that the cryptoasset was not obtained through illicit means. Such companies could also consider requiring customers to verify their purchases with a credit card or could impose a period of waiting time before payments are accepted so that the company can run checks on the customer's submitted compliance information (and potentially on-chain analysis of the digital wallet). A very cautious company might additionally require that purchasers' digital wallets be funded using centralized exchanges registered either in the company's home country or in a country with favorable discovery rules (to make third-party discovery easier in the event that problems do arise).

In light of the very specific risk that cryptoassets might have been used to evade U.S. economic sanctions, companies accepting cryptoassets should also remain vigilant about what they can do to ensure that they do not receive "criminally derived property" including property that was used to evade sanctions. Sanctions forfeiture laws are currently a subject of significant discussion at the DOJ, and U.S. Attorney General Merrick Garland recently proposed to "make it easier [for the DOJ] to do the forfeitures" as part of a

---

[44] See The 2021 Crypto Crime Report, supra note 1.

[45] 28 U.S.C. § 2462.

larger push to crack down on kleptocracy and sanctions evasion.[46] And the DOJ's new Task Force KleptoCapture is "fully empowered to use the most cutting-edge investigative techniques," including cryptoasset tracing, with a focus on seizing eligible assets even when arresting criminal suspects might otherwise be difficult.[47]

Part of the sanctions compliance analysis remains exactly the same for cryptoassets as it is for other assets—companies accepting cryptoassets should conduct KYC and due diligence processes on their customers, customer origination locations, etc., to screen for sanctions evaders, using the same analysis that has always applied to sanctions compliance in payment processing.[48] After all, even if a bona fide, innocent purchaser of an asset used to evade sanctions is allowed to keep that asset, the purchaser may still face a sanctions violation under OFAC's strict liability civil penalty regime for engaging in a sanctioned transaction.[49] This is why conducting pre-acquisition due diligence is of paramount importance.

However, the same characteristics of cryptoassets already discussed now require additional cryptoasset-specific analysis. For instance, because wallets are pseudonymized and could be used by multiple users without a clear and public attribution of ownership, companies should also do KYC and due diligence on the wallets from which they are receiving payments. Illustrating this point, OFAC's list of SDNs now includes not just the names of individuals, but also cryptoasset wallet addresses known or believed to be affiliated with those individuals.[50] A company proposing to receive payments from a wallet address

---

[46] Stewart Bishop, Garland Supports Legal Fixes To Go After Russian Oligarchs, Law360 (Apr. 26, 2022), https://www.law360.com/whitecollar/articles/1487040/garland-supports-legal-fixes-to-go-after-russian-oligarchs?nl_pk=563602ac-4590-4c78-934d-f1f5798f0aa4&utm_source=newsletter&utm_medium=email&utm_campaign=whitecollar&utm_content=2022-04-27.

[47] Id.; see also Press Release, U.S. Dep't of Just., Attorney General Merrick B. Garland Announces Launch of Task Force KleptoCapture (Mar. 2, 2022), https://www.justice.gov/opa/pr/attorney-general-merrick-b-garland-announces-launch-task-force-kleptocapture.

[48] This analysis should include, for instance, a comparison of all transacting parties against OFAC's list of Specially Designated Nationals (SDNs), who are prohibited transacting parties, requirements that users affirm that they are not located in prohibited jurisdictions (ideally with an IP address verification of their computer's location), representations by purchasers that they are not prohibited from engaging in the proposed transaction, and other proactive measures to avoid sanctions noncompliance.

[49] See 31 C.F.R. Part 501 App. A (Economic Sanctions Enforcement Guidelines).

[50] U.S. Dep't of Treasury, Cyber-related Designations and Designations Updates (Nov. 8, 2021), https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20211108; ICLG, Sanctions No End in Sight: An Update on the Rising Risk and Recent Developments in

must therefore—at a minimum—ensure that the wallet address is not on this list.

Companies expecting to earn significant sums of revenue in cryptoassets, however, are already doing more to ensure high levels of compliance. Yuga Labs (Yuga), for instance, the company behind the highly valued Bored Ape Yacht Club non-fungible token (NFT) collection,[51] recently partnered with Animoca Brands to launch an NFT project (Otherside.xyz), which generated an estimated $561 million dollars in retail sales within its first 24 hours.[52] However, despite operating in a market renowned for the anonymity of its participants (and despite having never implemented such a process on Yuga's previous NFT sales), Yuga and Animoca required every single party interested in participating in the sale to submit significant pre-transaction KYC information connecting their verifiable identity with the wallet they proposed to use to purchase the NFTs.[53] The required KYC information included scanned identity documents (passport, national ID, and driver's license), and submissions about full name, date of birth, address, proof of address, verifiable email address, verifiable Ethereum cryptoasset wallet address, and even a selfie photo to further prove the identity attribution.[54] This process is lengthy, tedious, and, most of all, expensive (to Yuga/Animoca) to deploy. But when the anticipated

---

Cryptocurrency Sanctions and Enforcement 2022 (Sept. 30, 2021), https://iclg.com/practice-areas/sanctions/2-no-end-in-sight-an-update-on-the-rising-risk-and-recent-developments-in-cryptocurrency-sanctions-and-enforcement.

[51] NFTs or "non-fungible tokens" are a specific category of cryptoasset that are unique from one another and may only ever be owned by a single wallet at a time (in contrast with fungible tokens such as ETH, the base token of the Ethereum block chain, for which each ETH is functionally equivalent to every other ETH, and any two ETH may be treated interchangeably from a value and exchange perspective). In the case of Bored Ape Yacht Club, the NFTs are 10,000 digital pictures of cartoon "apes" that confer access privileges to various token-gated community functions. Each ape is both artistically and cryptographically unique, and each has its own value proposition based upon its characteristics.

[52] Kate Irwin, Yuga Labs Sees $561 Million in Otherside Ethereum NFT Sales Within 24 Hours, DECRYPT (May 1, 2022), https://decrypt.co/99156/yuga-labs-sees-561-million-in-otherside-ethereum-nft-sales-within-24-hours.

[53] Owen Fernau, Crypto Balks at Bored Apes' KYC Requirement, THE DEFIANT (Mar. 12, 2022), https://thedefiant.io/bored-apes-kyc/; Bryan Teoh, BAYC x Animoca Brands' New Project Asks For Holders ID Causing Uproar, NFT EVENING (Mar. 16, 2022), https://nftevening.com/bayc-x-animoca-brands-new-project-asks-for-holders-id-causing-uproar/#:~:text=Yuga%20Labs%20and%20Animoca%20Brands,of%20joy%20on%20the%20streets; BAYC X Animoca KYC | Something Is Brewing You Just Have to Self Identify, NFT CULTURE (Mar. 11, 2022), https://www.nftculture.com/nft-news/bayc-x-animoca-kyc-something-is-brewing-you-just-have-to-self-identify/.

[54] Id.

proceeds reach into the hundreds of millions of dollars and when the goods being sold are valuable and easy to exchange, it is not a matter of whether people will try to use forfeitable funds to buy these products, it is only a matter of whether they will be successful and what a reasonable company would do in such circumstances to assure itself (and the government) that it is "reasonably without cause to believe that the property was subject to forfeiture."[55] Against this backdrop, and with hundreds of millions of dollars of revenue at stake, Yuga and Animoca decided that the cost of compliance (and the cost of demonstrating that the company is truly an innocent owner that took all reasonable steps) was simply the cost of doing its particular level of business in the cryptoasset/NFT space.

But not every company is expecting to take in hundreds of millions of dollars in revenue, and not every company is selling digital goods that are highly transferrable; not every company has the same risk calculus or compliance risk. Given the costs of these measures and the wide and diverse marketplace of goods and services for which cryptoassets could be exchanged, each company considering receiving cryptoassets for its products and services should instead do its own custom evaluation of its business model, its cryptoasset use case, and its potential forfeiture risk before it begins to accept cryptoassets. Doing so is not only prudent in light of the forfeiture risk posed by cryptoassets, but is also increasingly expected by both regulators and fellow market participants wishing to avoid similar pitfalls.

## CONCLUSION

The prospect of accepting cryptoassets presents plenty of potential benefits to businesses, and as the use of cryptoassets grows among the general populace, so too will customer demand that they be accepted as a form of payment. However, companies need to be aware of the risk of potential civil forfeiture actions stemming from accepting and holding cryptoassets, and need to take appropriate risk-mitigation steps to ensure the success of any endeavor to incorporate cryptoassets as payment.

To mitigate that risk, we advise that companies accepting cryptoassets set up procedures and policies to perform reasonable due diligence first on the history and characteristics of each cryptoasset they choose to accept, and second on the individuals and cryptoasset wallets with which they interact. This can be done either by hiring relevant in-house or external personnel capable of designing blockchain-specific (and ideally automated) compliance/KYC protocols, or in

[55] 18 U.S.C. § 983(d)(3)(A)(ii).

whichever way scales the due diligence to meet the specific company's risk of loss equal to the anticipated transactions' value. This judgment call will also relate to the size of the transactions at issue, the frequency with which such transactions are contemplated, and the kind of existing KYC, compliance, and due diligence functions the company already has in place. Only by conducting this appropriate level of due diligence will companies be able to ascertain with a reasonable degree of certainty whether they will be able to successfully assert, if necessary, the innocent owner defense.