CRYPTO CASE SUMMARIES

(April 1, 2024)

The following summaries were written by Stefan D. Cassella and are excerpted from the *Money Laundering and Forfeiture Digest,* a monthly publication of Asset Forfeiture Law, LLC.

Investment Fraud Cases

Bankman-Fried

Court sentences Bankman-Fried to 25 years in prison and imposes an $11 billion forfeiture money judgment, including $1 billion in specific assets.

United States v. Bankman-Fried, 2024 WL 1506561 (S.D.N.Y. Mar. 29, 2024).

S.D.N.Y. * Samuel Bankman-Fried, the founder of the failed cryptocurrency exchange FTX, was convicted of conspiracies to commit wire fraud, securities fraud, and money laundering and was sentenced to 25 years in prison. In addition, the court imposed an $11 billion forfeiture money judgment and forfeited a long list of specific assets that the court found to be the proceeds of the fraud offenses and property involved in the money laundering conspiracy.

The specific assets included the proceeds of the sale of 55 million shares of Robinhood Markets, Inc., which yielded $605 million in an interlocutory sale, $164 million in bank deposits, two airplanes, and a detailed list of 443 political contributions made by the defendant and his co-conspirators to named candidates for public office and political organizations. The forfeiture order was silent as to how the Government might go about recovering the political contributions.

The value of the specific assets, once they are liquidated (potentially $1 billion) will be credited toward the forfeiture money judgment, leaving the defendant personally liable for the remaining balance.

Contact: AUSA Samuel Raymond

Comment: As is so often the case, the media (including the New York Times and the Washington Post) reported only that the defendant was ordered “to pay” $11 billion, omitting that this was a judgment imposed under the criminal forfeiture laws. As we have observed many times – and pointed out to our friends in the media – reporters reserve the use of the term “forfeiture” for articles

criticizing law enforcement actions, and use “fine” or “payment” to refer to actions that are viewed as righteous or unexceptional. Why is that? *SDC*

Sharma

Judgment creditor lacks standing to contest the forfeiture of the defendant’s assets in the ancillary proceeding.

United States v. Sharma, 2021 WL 861353 (S.D.N.Y. Mar. 8, 2021).

S.D.N.Y. * Defendants pled guilty to a securities fraud scheme in which investors in cryptocurrency lost hundreds of millions of dollars, and agreed to the forfeiture of $36 million in cryptocurrency that was recovered. The court found that the number of potentially identifiable victims was so large as to make restitution impractical, but the Department of Justice agreed to dispense the forfeited funds to the victims on a *pro rata* basis through its remission process.

Claimants, representing a subset of the victims, were unhappy with this arrangement and filed a lawsuit against Defendants’ company. They obtained a default judgment and then filed a claim in the ancillary proceeding in Defendants’ criminal case asserting that the judgment gave them a superior interest in the forfeited funds. The Government responded by moving to dismiss Claimants’ claim for lack of standing.

The court held that as judgment creditors, Claimants had no interest in the specific units of cryptocurrency that were forfeited, and so lacked standing to contest the forfeiture in the ancillary proceeding. That the Government intends to use the proceeds of the sale of the forfeited cryptocurrency to compensate victims, the court said, does not mean that Claimants have the interest in specifically-identified property necessary to establish standing.

So, Claimants’ claim was dismissed. *SDC*

Contact: AUSA Negar Tekeei

Comment: It is well-established that to establish standing to contest the forfeiture of property in a criminal case, the claimant must show that he has an interest in the particular assets that have been forfeited, and is not merely an unsecured creditor of the defendant. A judgment creditor – that is, a person who has obtained a judgment against the defendant by filing a civil lawsuit – is no different from any other unsecured creditor until and unless he converts the judgment into a judgment lien against specific assets. The claimants in this case had not done that, and so they were unable to establish standing in terms of 21 U.S.C. § 853(n)(2).

Other cases denying claims filed by judgment creditors include *United States v. Catala*, 870 F.3d 6 (1st Cir. 2017) (creditor who obtained a judgment against defendant in state

court is still an unsecured creditor with no interest in the forfeited property); and *United States v. Madoff*, 2012 WL 1142292, *4 (S.D.N.Y. Apr. 3, 2012) ("To have a claim in the specific property, a creditor ... must secure a judgment or perfect a lien against a particular item"). *See also* Section XVIII.M.3 of the Criminal Forfeiture Case Outline. *SDC*

Sharma

Claims in the ancillary proceeding must be filed by individual claimants; the statute does not contemplate claims filed by a class of third parties under the procedures that would apply in a class action lawsuit.

Allowing a subset of investor-victims who can trace their losses to the forfeited property to claim the lion's share, while those who could not trace recovered nothing, would be unfair; the Government's plan to distribute all of the forfeited property to the victims on a pro rata basis through the remission process makes more sense.

United States v. Sharma, 2022 WL 1910026 (S.D.N.Y. Jun. 3, 2022).

S.D.N.Y. * Defendants pled guilty to a securities fraud scheme in which investors in cryptocurrency lost hundreds of millions of dollars, and agreed to the forfeiture of $36 million in cryptocurrency that was recovered. The court found that the number of potentially identifiable victims was so large as to make restitution impractical, but the Department of Justice agreed to dispense the forfeited funds to the victims on a pro rata basis through its remission process.

Claimants, representing a subset of the victims, were unhappy with this arrangement and filed a lawsuit against Defendants' company. They obtained a default judgment and then filed a claim in the ancillary proceeding in Defendants' criminal case asserting that the judgment gave them a superior interest in the forfeited funds. The Government responded by moving to dismiss Claimants' claim for lack of standing.

The court held that as judgment creditors, Claimants had no interest in the specific units of cryptocurrency that were forfeited, and so lacked standing to contest the forfeiture in the ancillary proceeding. So, the claim was dismissed. *United States v. Sharma*, 2021 WL 861353 (S.D.N.Y. Mar. 8, 2021) (April 2021 *Digest*).

Claimants, however, were unwilling to take 'no' for an answer. They filed a motion to file an amended claim arguing that they were the representatives of a class of victim-investors who could trace their lost investments to the forfeited cryptocurrency. The Government opposed the motion, arguing that even if Claimants could trace their lost investments to the forfeited property they still lacked standing as unsecured creditors. But the court did not reach that argument, finding other grounds on which Claimants motion should be denied.

First, the court held that the statute governing third-party claims in criminal forfeiture actions – 21 U.S.C. § 853 – "contemplates individual claimants making individual claims to property that otherwise would be forfeited." It does not contemplate class actions. Indeed, the court said, "the procedures contemplated by the forfeiture statute and F.R.Civ.P. 23(b)(3) [governing class actions] are fundamentally incompatible." For that reason alone, the court said, Claimants motion to file an amended claim should be denied.

Second, the court held that the proposed amended claim did not comport with the pleading requirements in Section 853(n)(3). It was not signed under penalty of perjury by each of the "thousands of class members" Claimants purported to represent, and it did not state the time and circumstances whereby each of the class members allegedly acquired an interest in the forfeited property.

Finally, the court held that the proposed amended claim would be prejudicial to the investor-victims who, unlike the members of the purported class, could not trace their losses to the forfeited property. If the amended claim were permitted and Claimants were to prevail, the court said, the victims who were outside of the class – *i.e.,* those who could not trace – "would receive virtually no recovery."

Moreover, the court concluded, the pool of assets available to the victims would be reduced by the attorney's fees (estimated to be as much as $6.6 million) that counsel to the class would take "off the top" before any distributions were made. In contrast, if the property were forfeited and the Government were permitted to distribute the money to the victims on a *pro rata* basis, all of the forfeited funds would go to the victims.

So, the motion for leave to file an amended claim on behalf of the victims who could trace their losses was denied. *SDC*

Contact: AUSA Negar Tekeei

Comment: It is not unusual for one set of victims in an investment fraud scheme – *i.e.,* those who can trace their losses to the forfeited property, a/k/a the "greedy victims" who want all of the recovered property for themselves – to make a claim in the ancillary proceeding of a criminal forfeiture case that, if successful, would be detrimental to the interests of the other victims who are not able to satisfy the tracing requirements. This case is unusual, however, for the manner in which the court disposes of the claim.

Generally, the argument goes like this: Victims who can trace file claims; Government argues that even though they can trace, they surrendered title to their property to the defendant and thus lack standing to contest the forfeiture. *See, e.g., United States v. BCCI Holdings (Luxembourg) S.A. (Final Order of Forfeiture and Disbursement*), 69 F. Supp. 2d 36, 59 (D.D.C. 1999) (a person who voluntarily transfers his property to the defendant is no longer the owner of that property; his ability to trace his property to the defendant's assets is irrelevant; therefore, victims who transferred their property to the

defendant have no greater standing to contest the forfeiture order than other unsecured creditors); *id*. 833 F. Supp. 9, 14 (D.D.C. 1993) (depositors' class action).

Victims then respond that they are actually the beneficiaries of a constructive trust, and so do have standing to contest the forfeiture of the property to which they can trace their losses. But the courts hold that a constructive trust is an equitable remedy that will not be imposed if the result would be prejudicial to similarly-situated parties – *viz.,* those who cannot trace. *See United States v. Andrews*, 530 F.3d 1232, 1238 (10th Cir. 2008) (district court did not abuse its discretion in refusing to impose a constructive trust on behalf of a victim who could trace his losses to the forfeited property where doing so would have been unfair to the victims who could not trace; in that situation, it is better to allow the Government to forfeit the property and distribute it to all of the victims on a pro rata basis).

None of those arguments were addressed by the court in this case, however, because it disposed of the proposed amended claim on other grounds: that class actions are not permitted in the ancillary proceeding; that each claimant in the ancillary proceeding must file an individual claim in accordance with § 853(n)(3); and – echoing the logic of the constructive trust cases – that it would be unfair to the victims who could not trace to allow a class of tracers to take the lion's share of the forfeited property. *SDC*

Sharma

Third parties who obtain a judgment lien against the defendant in a criminal case cannot use the lien to make a claim to the defendant's assets in the ancillary proceeding because the lien comes too late to defeat the Government's interest under the relation back doctrine.

Moreover, Congress made the ancillary proceeding the exclusive forum for litigating third party claims to the defendant's forfeited property precisely to avoid duplicative litigation.

A victim of the defendant's scheme to defraud cannot make a claim to the forfeited property as the beneficiary of a constructive trust if imposing the trust would be unfair to similarly situated third parties.

The property forfeited in a criminal case does not have to be property owned by the defendant; it is enough to show that the defendant exercised control over the property.

United States v. Sharma, 2023 WL 1365138 (S.D.N.Y. Jan. 31, 2023).

S.D.N.Y. * Defendants, the founders of the cryptocurrency firm Centra Tech,

pled guilty to a securities fraud scheme in which investors in cryptocurrency lost hundreds of millions of dollars. They agreed to the forfeiture of $33.4 million in cryptocurrency that was seized by the FBI from Centra Tech's digital wallet, and the Department of Justice agreed to dispense the forfeited funds to the victims on a pro rata basis through its remission process.

Claimants, representing a subset of the victims, were unhappy with this arrangement and filed a lawsuit against Defendants' company. They obtained a default judgment and then filed a claim in the ancillary proceeding in Defendants' criminal case asserting that the judgment gave them a superior interest in the forfeited funds. In the alternative, they argued that they should recover their losses from the forfeited funds because the court had improperly forfeited property that belonged to non-defendant Centra Tech, not to the individual defendants. Finally, they argued that because they could trace their losses, they were entitled to recover the property as the beneficiaries of a constructive trust.

The Government responded by moving to dismiss Claimants' claim under Rule 32.2(c)(1)(A) for failure to state a claim.

On the first point, the court held that Defendants' status as the holders of a judgment lien did not establish a basis to recover the forfeited property because the lien did not come into existence until after the Government's interest vested in the proceeds of the crime.

Under 21 U.S.C. § 853(n)(6)(A), which embodies the relation back doctrine, a third party claimant must show that his interest in the forfeited property arose *before* the Government's interest vested – which in the case of the proceeds of the defendants' crime was the moment the fraud occurred. Claimants' judgment lien came into existence long afterward, so it could not be the basis for a claim under Section 853(n)(6)(A).

Claimants responded that the default judgment in the civil suit should take priority over the ancillary proceeding, but the court held that Congress made the ancillary proceeding the exclusive forum for litigating third party claims to avoid "duplicative litigation," and that "allowing Claimants' judgment to establish superior claim on the seized assets through parallel litigation would frustrate the statutory scheme."

On the second point, the court held that it was appropriate to order the forfeiture of the $33.4 in cryptocurrency as part of Defendants' sentence because the funds were under Defendants' control. That Centra Tech, not Defendants, was the owner of the funds was not important.

Finally, the court acknowledged that a third party who could satisfy all of the elements of a constructive trust under state law might be able to satisfy the requirements of Section 853(n)(6)(A). But because a constructive trust is an equitable remedy, one of the requirements that a claimant must satisfy is that the imposition of the trust in his favor would not be detrimental to the interests of similarly situated third parties.

What Claimants were seeking, the court said, was to prioritize their claims over those of other investor-victims, including those who, unlike Claimants, could not trace their losses to the forfeited property. "Recognition of a constructive trust that would award Claimants more than their pro rata share as compared with other investors would be inequitable to other victims of Defendants' scheme."

So, the court held that none of Claimants' asserted grounds for recovery set forth a claim on which relief could be granted under Section 853(n)(6)(A), and accordingly, the Government's motion to dismiss was granted. *SDC*

Contact: AUSA Negar Tekeei

Comment: This was the third attempt by the claimants to recover their losses from the funds forfeited by the defendants in this case. In *United States v. Sharma*, 2021 WL 861353 (S.D.N.Y. Mar. 8, 2021), the court rejected their claim on the ground that they were merely unsecured creditors who lacked standing to contest the forfeiture of the defendants' assets. (April 2021 *Digest*) And in *United States v. Sharma*, 2022 WL 1910026 (S.D.N.Y. Jun. 3, 2022), the court rejected claimants' attempt to get around that troublesome standing rule by filing their claims not as individuals but as the representatives of a class. (July 2022 *Digest*). Now they try once again, asserting *inter alia* that they have an interest in the forfeited property as the beneficiaries of a constructive trust.

It is not unusual for one set of victims in an investment fraud scheme – *i.e.,* those who can trace their losses to the forfeited property, a/k/a the "greedy victims" who want all of the recovered property for themselves – to make a claim in the ancillary proceeding of a criminal forfeiture case that, if successful, would be detrimental to the interests of the other victims who are not able to satisfy the tracing requirements. Courts, however, universally reject the efforts of such "greedy victims" to assert they are the beneficiaries of a constructive trust.

In short, while the beneficiaries of a constructive trust might be able to recover in the ancillary proceeding in appropriate cases, no such trust will be imposed where the result would be detrimental to similarly situated victims of the defendant's crime. *See, e.g., United States v. Andrews*, 530 F.3d 1232, 1238

(10th Cir. 2008) (district court did not abuse its discretion in refusing to impose a constructive trust on behalf of a victim who could trace his losses to the forfeited property where doing so would have been unfair to the victims who could not trace; in that situation, it is better to allow the Government to forfeit the property and distribute it to all of the victims on a pro rata basis).

For other cases on this point as well as a thorough discussion of the role of a constructive trust civil and criminal forfeiture cases *see* § 23-15(g) of *Asset Forfeiture Law in the United States* (3d ed. 2022) and Section XX.H.2 of the Criminal Forfeiture Case Outline.

The court's treatment of the claimants' first argument – asserting their judgment lien as the ground for recovery – is also consistent with the universal view that to prevail under § 853(n)(6)(A), a third party must show that he had a pre-existing interest in the forfeiture property – a showing that a person whose interest in the property did not come into existence until he obtained a judgment lien generally cannot make. *See* Section XX.B.1 of the Criminal Forfeiture Case Outline. Nor, for that matter, could such a person establish the right to file a claim as bona fide purchaser for value under § 853(n)(6)(B) for the simple reason that obtaining a judgment lien is not a "purchase" within the meaning of the statute. *See United States v. Egan,* 654 Fed. Appx. 520 (2nd Cir. 2016) (person who obtains a judgment lien on the forfeited property is not a "purchaser" for purposes of § 853(n)(6)(B)), following *United States v. BCCI Holdings,* 69 F. Supp. 2d 36, 62 (D.D.C. 1999); *United States v. BCCI Holdings (Luxembourg) S.A. (Final Order of Forfeiture and Disbursement),* 69 F. Supp. 2d 36, 62 (D.D.C. 1999) ("A creditor who attempts to satisfy the debt by obtaining a judgment lien, or exercising a right of set-off, against specific property is not a bona fide purchaser of that property because he has given nothing of value in exchange for the property interest. This is so irrespective of how the antecedent debt came into existence."); *United States v. Bank,* 2022 WL 17477064 (E.D. Va. Dec. 6, 2022) (person who acquires a judgment lien on defendant's property without giving anything of value is not a "purchaser").

Finally, the court's rejection of the claimants' second argument – that the $33.4 million should never have been forfeited because it belonged to the defendants' corporation, not to the defendants personally – is interesting. I would have thought that the court would have dismissed that argument as one that a third party lacks standing to make. A third party can only use the ancillary proceeding to assert that the forfeited property belongs to him; he cannot use it to claim that there were defects in the proceeding that led to the forfeiture of the property. As the Tenth Circuit said in *Andrews,* "if the property really belongs to the third party, he will prevail and recover his property whether there were defects in the criminal trial or the forfeiture process or not; and if the property does not belong to the

third party, such defects in the finding of forfeitability are no concern of his." 530 F.3d at 1237.

But the court did not go in that direction. Instead, it addressed the claimants' objection on the merits and held that criminal forfeiture is *not* limited to property owned by the defendant, but may extend to property derived from the defendant's crime that is under his control, even if it is nominally owned by a third party such as a corporation. *See De Almeida v. United States,* 459 F.3d 377, 381 (2d Cir. 2006) (criminal forfeiture is not limited to property owned by the defendant; "it reaches any property that is involved in the offense;" *United States v. Watts,* 477 Fed. Appx. 816, 817-18 (2d Cir. 2012) (following *De Almeida;* property may be forfeited based on its nexus to the offense, regardless of ownership; the purpose of the ancillary proceeding is to allow third parties to challenge the forfeiture on ownership grounds); *United States v. Molina-Sanchez,* 298 F.R.D. 311, 314 (W.D.N.C. 2014) (because the property was derived from the offense for which the defendant was convicted, "the fact that defendant has no legal ownership interest in the . . . property does not bar criminal forfeiture"). *SDC*

Kwok

Court declines to release international fraudster and money launderer on bail, citing his ability to flee and to conceal assets, his technical sophistication involving the use of cryptocurrency, and the likelihood that he would continue to pose a risk of economic harm if released.

United States v. Ho Wan Kwok, 2023 WL 3027440 (S.D.N.Y. Apr. 20, 2023).

S.D.N.Y. * Defendant has been charged with defrauding thousands of victims of over $1 billion through an investment fraud scheme, and with laundering the proceeds through an international money laundering scheme. He was detained but filed a motion for release on bail pending trial.

The court held first that Defendant was a flight risk: He has bank accounts in several countries, eleven passports, and access to a yacht and a jet owned by family members. Moreover, the court said, the criminal charges provide "much incentive to flee."

Second, the court held that Defendant poses a risk of obstruction of justice. A court in a related bankruptcy case held that Defendant concealed assets; the victims in the pending case claim that Defendant has been harassing them on social media by "branding them 'spies' for the Chinese Communist Party;" and contrary to his

representation to Pretrial Services that he had no assets, a search revealed that Defendant had $500,000 in cash in a safe.

Moreover, the court said that Defendant was "technologically sophisticated." He has 17 computers and 30 cell phones; has previously advised followers on his website to use crypto currency services provided by one of his companies "to secure money against the long-arm jurisdiction of the United States;" and one of his co-conspirators was indicted for attempting to move fraud proceeds out of the U.S. after the Government began seizing assets from Defendant's businesses.

Finally, the court held that Defendant "poses a risk of economic harm to the community." When the SEC set up a fund for reimbursing Defendant's victims, he "encouraged them to re-invest their disbursements in the fraud scheme" – suggesting to the court that Defendant would continue to cause economic harm if released.

So, the motion for release on bail was denied. *SDC*

Contact: AUSA Juliana Murray

Scott

International wire fraud qualifies as a "specified unlawful activity" as long as some aspects of the fraud scheme -- beyond the incidental use of the wires -- were carried out in the United States.

To satisfy the knowledge requirement, the Government need only show that the defendant knew the property was derived from an international wire fraud scheme; he does not need to know that the particular funds he laundered came from U.S. victims.

United States v. Scott, 2023 WL 6064329 (S.D.N.Y. Sept. 14, 2023).

S.D.N.Y. * Defendant was the money launderer for an international Ponzi scheme based in Bulgaria that sold fake cryptocurrency to victims in the U.S. and elsewhere. He crafted an elaborate scheme for transferring proceeds of the scheme through foreign bank accounts and was found guilty by a jury of concealment money laundering; but he moved for a judgment of acquittal on several grounds.

First, he argued that the Ponzi scheme – which was alleged as a violation of the wire fraud statute -- was not a "specified unlawful activity" because it occurred largely outside of the United States, and wire fraud does not apply extraterritorially. But the

court held that because U.S. victims were targeted, and certain aspects of the scheme were carried out in the United States, the wire fraud offense qualified as an SUA.

Next, Defendant argued that the Government nevertheless had to prove that the money that he laundered was proceeds traceable to the U.S. victims of the offense. But the court held that even if there were such a requirement – which the court strongly doubted – the Government had offered evidence that money obtained from U.S. victims was included in the funds that Defendant laundered.

Third, Defendant argued that there was no evidence that he knew that the laundered funds were proceeds traceable to U.S. victims. But the court held that to satisfy the knowledge element, the Government need only show that the defendant knew that the property was derived from "some form of unlawful activity," and that because he was aware that the money came from an international fraud scheme, the element was satisfied.

Finally, Defendant argued that there was insufficient evidence that his transactions were designed to conceal or disguise. But the court noted that Defendant's layering funds through multiple international bank accounts and forging documents to obscure the paper trail between the Bulgarian fraudsters and the money that Defendant was placing in bank accounts in the Cayman Islands was more than sufficient to satisfy the concealment element.

So, Defendant's motion for a judgment of acquittal was denied. *SDC*

Crater

Court permits a Government expert to testify that a defendant's newly created cryptocurrency has never been traded on the public blockchain, allowing the jury to infer that it did not exist.

The inference that the cryptocurrency did not exist, and that customers who had been induced to purchase it had been defrauded, was not unfairly prejudicial to the defendant.

No Daubert *hearing is required before allowing a blockchain analyst to provide such testimony; her qualifications as an experienced analyst suffice to establish the admissibility of her testimony.*

United States v. Crater, 93 F.4th 581 (1st Cir. 2024).

First Circuit * Defendant advised investors that he had invented a new form of cryptocurrency called My Big Coin that was similar to Bitcoin but was superior in that it was backed by gold and was associated with Mastercard. Investors purchased at least $6.3 million in the new currency before discovering that it was not backed by gold, that there was no relationship to Mastercard, and that it could not be redeemed.

Defendant was charged with investment fraud and with operating an unlicensed money transmitting business. Prior to trial, the Government advised him that it planned to call a respected expert in blockchain analysis to testify that there was no evidence that Defendant's new cryptocurrency was ever traded on the public blockchain. Defendant objected that the proposed testimony unfairly implied that his cryptocurrency did not exist because it did not allow for the possibility that it was traded on a "private blockchain," and asked the court to hold a *Daubert* hearing on the admissibility of the expert testimony.

The court declined to hold the *Daubert* hearing and allowed the expert to testify. Defendant was convicted and appealed.

The panel held that the district court committed no error in declining to hold the *Daubert* hearing. The Government's expert, the court said, was well qualified to testify regarding how cryptocurrencies are traded on the public blockchain and to opine as to whether Defendant's cryptocurrency had ever been traded there. No hearing on the reliability of her methodology, the court said, was required before allowing the jury to hear her testimony.

As to Defendant's assertion that the expert did not allow for the possibility that his cryptocurrency was traded on a private blockchain, the panel endorsed the district court's view that that issue could be "fertile ground for cross-examination," but was not a reason to disallow the witness's testimony.

So, the court rejected Defendant's challenge to the expert testimony and affirmed his conviction. *SDC*

Contact: AUSA Christopher Markham (D. Mass.)

Ackerman

Third-party claim sent only to the U.S. Attorney's Office and not filed with the court until after the filing deadline is untimely and must be dismissed, even if the Government does not contest the claim on timeliness grounds.

A claim stating that the claimant received property purchased with criminal proceeds by quit-claim deed for no consideration does not state a claim on which relief can be granted under Section 853(n).

That the claimant paid for the maintenance of the property after receiving title to it makes no difference.

United States v. Ackerman, 2023 WL 3568654 (S.D.N.Y. May 18, 2023).

S.D.N.Y. * Defendant pled guilty to wire fraud involving a fraudulent cryptocurrency investment scheme and was ordered to forfeit a residence that he had purchased with fraud proceeds.

Claimant, the titled owner of the residence, filed a claim in the ancillary proceeding contesting the forfeiture on the ground that Defendant had quit-claimed the property to her (for no consideration) and that she had thereafter paid for the maintenance of the property with her own funds.

Although Claimant's attorney sent a copy of her claim to the U.S. Attorney within the time for filing a claim, she did not file it with the court until several months later.

The Government did not contest the claim on timeliness grounds, but did move under Rule 32.2(c)(1)(A) to dismiss it for failure to state a claim on which relief could be granted under 21 U.S.C. § 853(n).

The court held that notwithstanding the Government's acquiescence on the timeliness issue, the claim was filed out of time and "must be dismissed for that reason." Alternatively, it held that because Claimant did not allege that she gave anything of value in exchange for title to the property, she could not be a bona fide purchaser for value under Section 853(n)(6)(B), and therefore had not stated a claim on which relief could be granted.

So, the court granted the Government's motion to dismiss. *SDC*

Contact: AUSA Jessica Greenwood

Using Cryptocurrency to Launder Money

89.9270303 Bitcoins

Government's evidence that all of the cryptocurrency in a wallet was traceable to

access device fraud was sufficient to support summary judgment in a civil forfeiture case.

Claimant's argument that some of the cryptocurrency was derived from a legitimate source was insufficient to create a material issue of fact.

As to the cryptocurrency in a second wallet, the Government's "reasonable assumption" that it was derived from the first wallet is insufficient to support summary judgment without some evidence in the record tracing the contents of the second wallet to the first.

United States v. 89.9270303 Bitcoins, More or Less, 2021 WL 4307375 (W.D. Tex. Sept. 22, 2021).

W.D. Tex. * Defendant, an "asset protection" supervisor for Target stores, used his employee credentials to access Target's gift card database. He stole more than $115,000 in value from the gift cards, converting the money to Bitcoins that he held in a cryptocurrency wallet.

When Defendant was arrested, he gave his attorney access to the cryptocurrency wallet. The attorney conducted a series of transactions involving that wallet before turning it and two other wallets over to the Government. The Government then filed a civil forfeiture action against all three wallets, alleging that they contained the proceeds of access device fraud.

Defendant filed a claim in the civil forfeiture action and opposed the Government's motion for summary judgment. He argued that while some of the Bitcoins in the first wallet were traceable to his offense, the balance was not. He also argued that the Government could not prove that the second and third wallets turned over by his attorney were traceable to the first wallet.

The court found that the Government's evidence was sufficient to prove, by a preponderance of the evidence, that all of the contents of the first wallet were traceable to the access device offense. Defendant's assertion to the contrary, the court said, was insufficient to establish an "innocent owner defense."

With respect to the second and third wallets, however, the court agreed with Defendant that the evidence in the record was insufficient to establish that the money turned over by the attorney was traceable to the offense. Given the timing of the attorney's actions, the court said, the Government's assumption that all of the cryptocurrency turned over by the attorney was forfeitable was "reasonable." But for purposes of summary judgment, what the Government needed to do was to submit an affidavit or similar admissible evidence explaining that what the attorney had turned

over was in fact taken from the first wallet.

So, the Government's motion for summary judgment was granted as to the money in the first wallet, and denied as to the money in the second and third wallets. *SDC*

Contact: AUSA Mary Valadez

Comment: As to the first wallet, the court characterizes the defendant's failure to prove that at least a portion of the cryptocurrency was derived from a legitimate source as a failure to meet his burden of proof on the innocent owner defense. With all due respect, the defendant's argument that some of the cryptocurrency was not an assertion of the innocent owner defense, *see* 18 U.S.C. § 983(d), but a refutation of the Government's proof that *all* of the cryptocurrency was subject to forfeiture.

This is important, because while the claimant in a civil forfeiture action bears the burden of proof on the innocent owner defense, he has no such burden with respect to the forfeitability of the property. To the contrary, Government at all times bears the burden of proving forfeitability by a preponderance of the evidence.

In granting the Government's motion for summary judgment, what the court was properly holding was not that the defendant failed to establish an innocent owner defense, but that he had failed to show the existence of a material issue of fact regarding the illicit source of the property. Viewed that way, the entry of summary judgment for the Government as to the first wallet was entirely correct. *SDC*

89.9270303 Bitcoins

Court permits the Government to take the deposition of the attorney who handled claimant's cryptocurrency accounts when he represented him in his criminal case to assist in determining which assets were traceable to claimant's offense.

United States v. 89.9270303 Bitcoins, More or Less, 2022 WL 432562 (W.D. Tex. Feb.11, 2022).

W.D. Tex. * Claimant, an "asset protection" supervisor for Target stores, used his employee credentials to access Target's gift card database. He stole more than $115,000 in value from the gift cards, converting the money to Bitcoins that he held in a cryptocurrency wallet.

When Claimant was arrested, he gave his criminal defense attorney access to the cryptocurrency wallet. The attorney conducted a series of transactions involving

that wallet before turning it and two other wallets over to the Government. The Government then filed a civil forfeiture action against all three wallets, alleging that they contained the proceeds of access device fraud.

Claimant filed a claim in the civil forfeiture action and opposed the Government's motion for summary judgment. He argued that while some of the Bitcoins in the first wallet were traceable to his offense, the balance was not. He also argued that the Government could not prove that the second and third wallets turned over by his attorney were traceable to the first wallet.

The court found that the Government's evidence was sufficient to prove that all of the contents of the first wallet were traceable to the access device offense. With respect to the second and third wallets, however, the court agreed with Claimant that the evidence in the record was insufficient to establish that the money turned over by the attorney was traceable to the offense. So, the Government's motion for summary judgment was granted as to the money in the first wallet, and denied as to the money in the second and third wallets. *United States v. 89.9270303 Bitcoins, More or Less,* 2021 WL 4307375 (W.D. Tex. Sept. 22, 2021) (November 2021 *Digest*).

The court then permitted the Government to take the deposition of the attorney, and based on his testimony, it renewed its motion for summary judgment as to the remaining assets. The court held, however, that while the testimony was sufficient to establish the forfeitability of some of the remaining assets, it left open the possibility that other assets had been in Claimant's possession before he committed the gift card offense.

So, once again, the court granted the Government's motion for summary judgment in part and denied it in part. *SDC*

Contact: AUSA Mary Valadez

Guerrero

Venue for a money laundering conspiracy is proper in any district where any member of the conspiracy committed an overt act.

Money launderers may be charged with engaging in a single conspiracy if they act with the common purpose of laundering drug proceeds, even if they do not know each other.

The Government is not required to name the co-conspirators with whom the defendant conspired in the indictment.

United States v. Guerrero, 2022 WL 2079861 (E.D. Ky. Jun. 9, 2022), and *United States v. Guerrero,* 2022 WL 2165908 (E.D. Ky. Jun. 15, 2022).

E.D. Ky. * Defendant was charged with a money laundering conspiracy in the Eastern District of Kentucky. He argued that venue was improper in that district because he had never been there; all of his alleged acts, he said, occurred in the Northern District of Illinois.

Pursuant to 18 U.S.C. § 1956(i)(2), venue for a money laundering conspiracy lies in any district where any member of the conspiracy committed an overt act. Because Defendant's co-conspirators made phone calls arranging for the delivery of drug proceeds to undercover agents in the district, the court said, and later arranged for the conversion of those proceeds to Bitcoin in the district and their transfer to cryptocurrency wallets, Defendant could be tried in the Eastern District of Kentucky even though he personally committed no acts there.

Defendant responded that the overt acts of his co-conspirators could support venue only if those acts were all part of a single conspiracy. In this case, he argued, what took place in Kentucky and what took place in Illinois were parts of separate conspiracies. But the court held that because the co-conspirators acted with a common purpose – to launder drug proceeds for one or more drug organizations – they were participants in a single conspiracy even if they did not know each other.

So, Defendant's motion for a change of venue to the Northern District of Illinois was denied.

Separately, Defendant filed a motion *in limine* to exclude the statements of his alleged co-conspirators. But the court, having held that Defendant and the co-conspirators engaged in a single conspiracy, held that the co-conspirator statements were admissible under F.R.Evid. 801(d)(2)(E).

Finally, Defendant asked the court to order the Government to reveal the identities of the co-conspirators with whom he allegedly conspired to commit the money laundering offense. The Government opposed the motion, arguing that it did not want to reveal the names of indicted conspirators who were fugitives until they were arrested.

The court held that a defendant may be indicted and convicted of a conspiracy despite the names of his co-conspirators remaining unknown as long as the Government proves that there was a conspiracy. Accordingly, the court held that it was

not necessary for the Government to identify the co-conspirators by name in the indictment. *SDC*

Contact: AUSA Gary Bradbury

Comment: The cases holding that venue for a money laundering conspiracy lies in any district where any of the co-conspirators committed an overt act are collected in Section XXXIV.F of the Money Laundering Case Outline. *SDC*

Iossifov

Venue for a money laundering conspiracy is proper in any district where any member of the conspiracy committed an overt act; that the defendant, who was one of the conspirators, never entered the United States makes no difference.

Under Section 1956(f), the extraterritoriality provision applies to all defendants who joined a money laundering conspiracy that occurred in part in the United States, including a defendant whose only act was to launder the proceeds in Bulgaria.

Evidence that defendant's Bitcoin exchange business had laundered fraudulently derived Bitcoin for other customers on other occasions was admissible under Rule 404(b) because it shed light on defendant's knowledge of the illicit source of the money.

In determining on appeal whether there was sufficient evidence of the defendant's knowledge of the illegal source of the money, the jury's rejection of the defendant's testimony to the contrary cannot be lightly disregarded.

At sentencing, the district court properly applied the 2-level obstruction enhancement to defendant who took the stand and lied as to whether he enforced the AML/KYC policies of his Bitcoin exchange business.

Bitcoins constitute "funds" for purposes of the money laundering statute.

United States v. Iossifov, 45 F.4th 899 (6th Cir. 2022).

Sixth Circuit * A criminal organization based in Romania induced nine hundred victims – mainly in the United States – to send them money for non-existent goods that were advertised for sale on the internet. The organization laundered the money twice: first in the United States by having third parties convert it to Bitcoin and transfer it to Romania,

and second by having Defendant's Bitcoin exchange business in Bulgaria convert the Bitcoin back to fiat currency.

Defendant was convicted by a jury of RICO and money laundering conspiracies and appealed, raising a host of objections to his conviction and sentence. A Co-Defendant who was part of the first phase of the money laundering in the United States pled guilty but appealed his sentence.

First, Defendant – who claimed that he had never set foot in the United States -- objected to venue in the Eastern District of Kentucky and to the application of the extraterritorial provision of the money laundering statute. The court held, however, that venue was proper because other members of the conspiracy had committed overt acts in Kentucky, and that the conspiracy fell within the scope of 18 U.S.C. § 1956(f) – the extraterritorial provision of the money laundering statute – which gives the district courts jurisdiction over any act that occurs at least part in the United States.

Because the first phase of the money laundering conspiracy – the conversion of the victims' funds to Bitcoin – occurred in the United States, the court said, the extraterritorial provision applied.

Defendant argued that if that was so, Section 1956(f) was unconstitutional as it applied to him – a person not involved in the acts that occurred in the United States. But the court held that the acts committed in the United States were so extensive, and Defendant's collaboration in the conspiracy so significant, that it was not "fundamentally unfair" to find that Defendant fell within the scope of the extraterritoriality statute.

Next, Defendant argued that Bitcoin are not "funds" for purposes of the money laundering statute. But the court held otherwise, collecting the case law on that point.

Defendant next claimed there was no evidence that he knew that the funds he was converting from Bitcoin to fiat currency in Bulgaria represented fraud proceeds. But the court found ample direct and circumstantial evidence to support the jury's verdict on that point.

Among other things, the court noted that co-defendants testified that Defendant was aware of the source of the money; that emails showed that Defendant never followed the anti-money laundering (AML) policies that his company purported to follow; and that Defendant acquiesced in a co-defendant's request that he provide him with fiat currency "in a paper bag."

Moreover, Defendant took the stand in his own defense and claimed that he had no knowledge of the illegal source of the money. The jury's decision not to believe Defendant, the court said, may not lightly be disregarded on appeal.

Defendant's final challenge to his conviction concerned the district court's admission of evidence that Defendant had laundered tainted funds for other criminals on other occasions. That evidence, Defendant said, was not admissible under F.R.Evid. 404(a). But the court held that the evidence that Defendant had laundered money for others in similar circumstances was admissible under Rule 404(b) because it "shed direct light upon [Defendant's] understanding and conscious knowledge" that his business was engaged in the exchange of fraudulently obtained Bitcoin.

Finally, Defendant challenged the calculation of his offense level under the Sentencing Guidelines, arguing that the court improperly imposed a 2-level enhancement for obstruction of justice, and improperly attributed the laundering of $4.9 million to him.

On the first point, the court held that Defendant's testimony under oath that he enforced the AML policies of his company by, *inter alia*, asking his customers for their identification – testimony that was contradicted by numerous witnesses – was sufficient to support the obstruction enhancement.

On the second point, the court held that "relevant conduct" – including the amounts laundered by Defendant's customers through his Bitcoin exchange business – was the appropriate measure of the amount attributable to him for purposes of calculating his offense level.

The Co-Defendant who pled guilty to laundering the victims' funds at the "front end" of the conspiracy similarly contested the calculation of the amount attributable to him for sentencing purposes. Personally, he said, he laundered only $664,000. But the court held that the "relevant conduct" in Co-Defendant's case included the $2.74 million that other members of the conspiracy laundered in the Eastern District of Kentucky.

So, Defendant's conviction was affirmed, as were Defendant's and Co-Defendant's sentences. *SDC*

Contact: DOJ Attorney Ann Adams and AUSA Charles Wisdom (E.D. Ky.)

Comment: This case touches on a great many issues – too many to comment on each one. So, I will simply direct the reader to other cases on some of the most important points.

With respect to the venue issue, other cases holding that venue for a money laundering conspiracy is proper under Section 1956(i)(2) in any district where any member of the conspiracy committed an overt act are collected in Section XXXIV.F of the Money Laundering Case Outline and § 9.6.3 of *Federal Money Laundering: Cases and Forfeitures* (2d ed. 2021).

Other cases on extraterritoriality under § 1956(f) are collected *id.* in §§ XXXIII.A and 9.7, respectively. The defendant's argument that § 1956(f) violated his right to due process because he was in no way involved in the acts that occurred in the United States was rejected on the merits – there was ample evidence that Defendant was intimately involved in many aspects of the fraud scheme; but the court left open the possibility of such a due process challenge to § 1956(f) on other facts.

The cases on the circumstantial evidence that may be used to establish that a defendant knew that he was laundering criminal proceeds are collected *id.* in §§ VII.I and 5.1.3.7, respectively.

Finally, the cases on the application of the obstruction of justice enhancement and the amount of laundered funds attributable to the defendant are collected in §§ XXIX.V and 10.1.6, respectively. *SDC*

Chastain

United States v. Chastain, 2022 WL 13833637 (S.D.N.Y. Oct. 21, 2022).

S.D.N.Y. * Defendant was charged with profiting from the misappropriation of confidential business information and with concealing the proceeds by "transferr[ing] funds through anonymous Ethereum blockchain accounts and new Ethereum accounts without any prior history," in violation of the concealment money laundering statute. He moved to dismiss the indictment, arguing that doing what was alleged, even if true, would not constitute concealment. But the court held that that was a question for the jury and denied the motion.

Contact: AUSA Thomas Burnett

Chastain

United States v. Chastain, 2023 WL 2966643 (S.D.N.Y. Apr. 17, 2023).

S.D.N.Y. * The Government opposed Defendant's request to present an expert witness at his trial for laundering the proceeds of a wire fraud scheme by transferring funds through anonymous Ethereum blockchain accounts. The court held that the witness could not offer an opinion as to whether Defendant's conduct constituted money laundering or whether Defendant acted with the state of mind necessary to establish a money laundering offense; but the witness could testify generally about the technologies that Defendant used, what the common practices are with respect to such technologies, and the extent to which those technologies do or do not conceal a person's identity or conduct.

Contact: AUSA Thomas Burnett

Crypto-Laundering Facilitators

Sterlingov

Clean money used to facilitate a money laundering offense is forfeitable as property 'involved in' money laundering; therefore, even if some of the money commingled with the funds being laundered in defendant's bitcoin tumbling operation were legitimately derived, they were subject to forfeiture.

Similarly, funds that defendant commingled with other funds in his operation of an unlicensed money transmitting business were subject to forfeiture as property involved in the violation of § 1960, regardless of how they were initially obtained.

After applying the Jones-Farmer *rule, and finding that defendant lacks other funds with which to retain counsel, the court puts the burden on the Government to defend the probable cause finding that was made by the judge who issued the seizure warrant for defendant's property, and finds that it has done so.*

United States v. Sterlingov, 2023 WL 2387759 (D.D.C. March 6, 2023).

D.D.C. * Defendant operated Bitcoin Fog, a bitcoin tumbling business that commingled bitcoin from different customers in a pooled account and then redistributed them to the customers, minus a fee. In so doing, Defendant's business made it difficult for law enforcement to trace a given quantity of bitcoin to its original source.

Defendant was indicted for conspiracy to commit money laundering and for operating an unlicensed money transmitting business, in violation of 18 U.S.C. §§ 1956(h) and 1960, respectively. The Government also obtained a warrant to seize cash and various cryptocurrencies from Defendant's accounts at a digital currency exchange known as Kraken, alleging that the funds were subject to forfeiture under 18 U.S.C. § 982(a)(1) as property involved in the money laundering and money transmitting business offenses.

Defendant admitted that the money seized from the Kraken accounts came from Bitcoin Fog, but he nevertheless argued they were derived from legal activity – such as his investment in cryptocurrency -- not from fees he earned from operating the business illegally as alleged in the indictment. Accordingly, he argued that there was no probable cause for the seizure, and that the funds should be released so that he could use them to pay his defense attorney.

The court acknowledged that under the D.C. Circuit's version of the *Jones-Farmer* rule, defendant had to show that he lacked other funds with which to retain counsel. But it found that Defendant satisfied that requirement, and accordingly afforded Defendant a probable cause hearing, at which the Government had the burden of defending the probable cause for the seizure warrant.

At the hearing, Defendant repeated his asserted that the activities in which his business engaged were not illegal, and that in any event, the funds that the Government seized, while coming from the business, were derived from legitimate activities. But the court rejected both arguments.

Under the Supreme Court's decision in *Kaley,* the court said, a defendant who satisfies the requirements for a pre-trial probable cause hearing may challenge the probable cause for the forfeitability of his property, but may not challenge the grand jury's finding of probable cause regarding his commission of the underlying crime. Thus, for purposes of the hearing, Defendant could not challenge the grand jury's finding that his business was an unlicensed money transmitting business engaged in the laundering of criminal proceeds. He could only contest the forfeitability of the funds that he transferred from that business to his Kraken account.

On that issue, the court held that it was irrelevant whether the funds Defendant transferred from his business were legitimately derived funds or the commissions he earned from laundering money for his clients.

Untainted funds that are commingled with other funds for the purpose of facilitating a money laundering offense, the court said, are forfeitable as property involved in money laundering. Therefore, because Defendant commingled his funds with the funds from his clients in the alleged tumbling operation, there was probable cause to believe that they were subject to forfeiture as facilitating property regardless of how Defendant had acquired them.

Similarly, with respect to the Section 1960 violation, the court held that because Defendant's funds in Bitcoin Fog "were intermingled (or tumbled) with other funds" – and thus "facilitated its operations" -- *all* of the funds were subject to forfeiture as property 'involved in' the operation of an unlicensed money transmitting business "irrespective of how the funds were initially procured."

Accordingly, the court held that there was probable cause to forfeit the seized funds as property involved in the violations of Sections 1956 and 1960 and denied Defendant's motion to release the funds. *SDC*

Contact: AUSA Chris Brown

Comment: This opinion addresses and collects the cases on a number of important issues.

First, it holds that the *Jones-Farmer* rule applies in the D.C. Circuit, and that once the defendant makes the showing that he lacks other funds with which to retain counsel, the Government bears the burden of "defending" the probable cause funds that was made by the magistrate judge who issued the seizure warrant.

Next, it collects the cases holding that untainted funds that are used to facilitate a money laundering offense through commingling are forfeitable as property involved in money laundering. In particular, it holds that "when a money laundering conspiracy takes the form of a business, all funds flowing through the business that 'bankroll' or otherwise facilitate the alleged conspiracy are 'involved in it' and may be restrained."

Finally, it collects the far smaller number of cases holding that all funds moving through an unlicensed money transmitting business are forfeitable as property involved in a violation of § 1960. *SDC*

Harmon

United States v. Harmon, 2020 WL 2299970 (D.D.C. Apr. 29, 2020).

D.D.C. * A district court issued a pre-trial restraining order pursuant to 21 U.S.C. § 853(e)(1)(A) directing the defendant to provide the Government with access to all cryptocurrency within his possession "by disclosing seed recovery keys, access to hidden wallets, and other keys needed to transfer cryptocurrency." It further ordered that the Government should "securely store" the cryptocurrency by transferring it to the US Marshals Service.

Contact: AUSA Chris Brown

Comment: The Government's request for the restraining order, setting forth the logistical issues involved in restraining cryptocurrency, is posted in the Brief Bank on my website, www.assetforfeiturelaw.us. *SDC*

Harmon

Court rejects void-for-vagueness challenge to Section 1960 as applied to a business that "tumbles" bitcoins to conceal their source and ownership.

United States v. Harmon, 2021 WL 1518344 (D.D.C. Apr. 16, 2021).

D.D.C. * Defendant operated an online service known as a "bitcoin tumbler." Customers would send him bitcoins and Defendant would "tumble" them with bitcoins from other customers, thereby stripping the bitcoins of information linking them to their owner. He advertised this service as "a way to conceal transactions from law enforcement."

An indictment charged Defendant, *inter alia,* with operating a money transmitting business without a state license and without registering with FinCEN, in violation of 18 U.S.C. § 1960(b)(1)(A) and (B), respectively. In an earlier case, the court rejected Defendant's motion to dismiss those counts on the ground that bitcoins are not "money," and that tumbling bitcoins is not a "money transmitting business." *United States v. Harmon,* 474 F. Supp.3d 76 (D.D.C. 2020).

Defendant nevertheless renewed his motion arguing that even if the court were correct on those two points, the statute was so vague that it deprived him of his due process right to fair notice that his conduct was illegal. The court did not agree.

On the first point, the court held that the statutory language gave a person of ordinary intelligence fair notice that "bitcoin falls under the ordinary meaning of the word 'money'."

On the second point, Defendant pointed to the absence of any federal regulation specifically including "bitcoin-to-bitcoin swapping" within the meaning of "money

transmitting business," articles written by "bitcoin enthusiasts" that gave "no indication that tumbling bitcoin could be a potentially illegal act," and the absence of any prior criminal prosecution of a bitcoin tumbler. But the court was unimpressed.

FinCEN guidance predating the operation of Defendant's business, the court said, defined "money transmitting business" to include the transfer of virtual currency from one person to another. This includes a bitcoin tumbler who "works by literally mixing up a user's payment with lots of other payments from other users."

Regarding Defendant's reference to published articles, the court observed that "bitcoin industry enthusiasts are woefully unpersuasive as authorities on the legality of bitcoin tumbling operations."

Finally, the court held that the fact that "this is the first U.S. prosecution of a cryptocurrency mixer does not, standing alone, render a statutory application so novel as to be unconstitutional for vagueness."

So, Defendant's motion to dismiss the Section 1960 counts from his indictment was denied. *SDC*

Contact: AUSA Chris Brown

Phillips

The exchange of Bitcoin for cash is a "financial transaction" for purposes of the money laundering "sting" statute.

United States v. Phillips, 2022 WL 16990050 (W.D.N.Y. Nov. 17, 2022).

W.D.N.Y. * Defendant met with an undercover agent who told him that he wanted to exchange Bitcoin for currency "so that it would appear clean." On five occasions, the agent transferred Bitcoin from a digital wallet to a digital wallet address provided by Defendant, who gave the agent a box of currency in return, promising not to file any reports of the currency transactions.

In the course of these meetings, the agent told Defendant that the Bitcoin was the proceeds of "ID theft, hacking, and selling cocaine."

Defendant was ultimately arrested and charged with five counts of money laundering under the "sting" statute, 18 U.S.C. § 1956(a)(3)(B) and (C). He moved to dismiss the indictment on the ground that exchanging Bitcoin for cash is not a "financial transaction" within the meaning of Section 1956(c)(4).

The court did not agree. First, the court joined all others that have considered the issue and held that Bitcoin are "funds" within the meaning of Section 1956(c)(4)(A)(i), and rejected Defendant's contrary view that they are a commodity. That the IRS treats cryptocurrency as a commodity for tax purposes, the court said, does not "illuminate the meaning of 'funds' in the federal criminal money laundering statutes."

Second, the court held that even if Bitcoin are not "funds", the exchanges of cryptocurrency for cash that occurred in this case would nevertheless qualify as financial transactions because the cash is a monetary instrument within the meaning of Section 1956(c)(4)(A)(ii).

Defendant disputed that point, arguing that a transaction is a "financial transaction" within the meaning of paragraph (A)(ii) only if the "monetary instrument" involved in the transaction represents the SUA proceeds being laundered. But the court held that there is no such limitation in the statute.

When the transaction involves the exchange of one thing for another, it does not matter which thing is the monetary instrument and which is the SUA proceeds. If Defendant's interpretation were correct, the court concluded, the exchange of stolen merchandise for cash would not be a "financial transaction" within the meaning of the money laundering statute because the cash would be the monetary instrument and the merchandise the SUA proceeds.

So, Defendant's motion to dismiss the indictment was denied. *SDC*

Contact: AUSA Kyle Rossi

Comment: In holding that Bitcoin are "funds" for purposes of the money laundering statute, the court follows the Sixth Circuit's recent decision in *United States v. Iossifov,* 45 F.4th 899 (6th Cir. 2022), and held that its reasoning applies equally to the "sting" provision in § 1956(a)(3). It also collects the wealth of district court cases holding that cryptocurrencies are "funds." *SDC*

Freeman

A bitcoin exchange business that exchanges fiat currency for bitcoin must register with FinCEN as a money transmitting business.

Person who maintains bitcoin exchange machines cannot be found guilty of participating in the conduct of a money laundering transaction conducted by a customer

without proof that he knew that a particular transaction was taking place; that he maintained the machines and told the customer how to use them is not enough.

United States v. Freeman, 2023 WL 5391417 (D.N.H. Aug. 22, 2023).

D.N.H. * Defendant ran a bitcoin exchange business in which he charged customers a fee for exchanging fiat currency for bitcoin. Customers could use Defendant's website to wire fiat currency to Defendant's bank accounts and receive bitcoin in private digital wallets in return. Or they could use bitcoin exchange machines that Defendant placed in local bars and similar establishments to do the same thing.

On one occasion, an undercover agent (UCA) who had been trading dollars for bitcoin through the website, met with Defendant and asked about conducting transactions through the machines with money from his illegal drug business. Defendant described the process but was not present when, sometime later, the UCA conducted an $11,000 transaction through one of the machines, receiving bitcoin minus Defendant's transaction fee in return.

Defendant was convicted by a jury of conducting an unlicensed money transmitting business in violation of 18 U.S.C. § 1960 and of conducting a concealment money laundering offense under the sting statute, 18 U.S.C. § 1956(a)(3)(B). He then moved for a judgment of acquittal.

Defendant's argument with respect to the Section 1960 violation was that the statute does not apply to bitcoin exchanges because bitcoins are not "funds." Moreover, he argued that to the extent the Government was relying on FinCEN regulations defining "funds" to include bitcoins, it was improper to do so because FinCEN lacked authority from Congress to deal with such a "major question" by regulation.

The court held, however, that both Section 1960 and 31 U.S.C. § 5330 (which supplies the definition of "money transmitting business" on which Section 1960 relies) apply unambiguously to bitcoin exchanges because bitcoins are "funds." Therefore, there was no need for the Government to rely on the FinCEN regulations to establish that Defendant had violated the statute. But even if the statutes themselves were ambiguous on this point, the court said, defining "funds" to include bitcoins was not a "major question" that fell outside of FinCEN's authority to issue regulations.

The court then turned to Defendant's conviction under the sting statute for conducting the transaction that the UCA processed through Defendant's bitcoin exchange machine.

To prove a violation of the statute, the court said, the Government must prove that the defendant "conducted" the transaction. While this does not require proof that

the defendant conducted the transaction personally – one can "conduct" a transaction by causing another person to take the steps necessary to initiate or conclude it – the Government must prove, at a minimum, that the defendant knew that the transaction was being conducted.

Here, notwithstanding the evidence that Defendant had given the UCA the green light to conduct the $11,000 transaction at the bitcoin exchange machine, there was no evidence showing that he knew that the UCA had actually done so. For example, there was no evidence that Defendant was present when the UCA went to the bar to use the machine, that the agent told him that he had done so afterwards, or that Defendant was monitoring all transactions through the machine.

Accordingly, the court denied the motion for judgment of acquittal on the Section 1960 count, but granted it with respect to the money laundering count for failure to prove that Defendant had "knowingly" conducted the financial transaction. *SDC*

Contact: AUSAs Georgiana MacDonald and Seth Aframe

Comment: To prove a violation of Section 1956(a)(3), the Government must prove that the defendant conducted a financial transaction. Section 1956(c)(1) defines "conducting a financial transaction" broadly to include participating in initiating or concluding a transaction. Thus, it is clear that the defendant does not have to conduct the transaction personally, but may be found criminally liable if, for example, he takes part in arranging for an undercover agent to conduct the transaction. *See United States v. Kiselev, supra* (defendant could be charged with money laundering in N.D. Cal. because he agreed that undercover agent would send sting money from San Francisco to defendant's bank account).

The problem in this case, however, was not that the defendant did not conduct the transaction personally; it was that there was no proof that he knew the transaction was conducted at all.

The statute requires proof that the defendant "knowingly" conducted a financial transaction. But one cannot knowingly conduct a transaction if he does not know that the transaction is being conducted!

Here, all the Government could show was that the defendant maintained bitcoin exchange machines, that he knew a customer (the UCA) wanted to use the machines, and that he explained to the customer how to do so. But the Government could not show that the defendant knew that the customer had followed through on his plan and actually used the machine. That the customer did so was not enough; there had to be proof that the defendant knew it.

What this suggests is that the Government cannot convict a person of money laundering just because he provided the means of conducting transactions through automated machines and knew that one or more of his customers intended to use them to conduct transactions involving criminal proceeds. Fair enough; but other courts have held that one who provides the means by which customers can commit money laundering offenses may himself be convicted of a *conspiracy* to commit such offenses. *See United States v. Ulbricht,* 2014 WL 3362059, *11 (S.D.N.Y. July 9, 2014) (setting up an online marketplace with the specific intent to facilitate the anonymous laundering of criminal proceeds may be charged as a money laundering conspiracy). *SDC*

Binance

Binance pleads guilty to conducting an illegal money transmitting business, failing to maintain an effective AML/KYC program, and knowingly allowing its customers to violate IEEPA by sending money to Iran.

As part of its plea, the company agrees to forfeit $2.5 billion in criminal proceeds.

United States v. Binance Holdings Limited, 23-Cr-178-RAJ (W.D. Wash. Nov. 14, 2023).

W.D. Wash. * Binance.com, one of the world's largest cryptocurrency exchanges, pled guilty to a three-count criminal information charging it with failing to register as a money service business in violation of 18 U.S.C. § 1960, failing to maintain an effective Anti-Money Laundering / Know Your Customer (AML/KYC) program in violation of 31 U.S.C. § 5318(h), and conducting financial transactions between U.S. persons and sanctioned countries in violation of the International Emergency Economic Powers Act (IEEPA), 50 U.S.C. § 1705.

As part of the plea agreement, the company agreed to pay a $1.8 billion criminal fine and to forfeit $2.5 billion in connection with the Section 1960 and IEEPA offenses.

The Government alleged that Binance.com, as a foreign-based money service business, was required to register with FinCEN because a substantial part of its customer base was in the United States. The company attempted to circumvent the registration requirement by creating a U.S.-based subsidiary, Binance.US, that did register with FinCEN, and by shifting its low volume customers to that platform, but it retained its high-volume U.S. customers on Binance.com, and encouraged them to disguise their U.S. connection by changing their KYC information to foreign-based entities with foreign IP addresses. This subterfuge was discovered and led to the Section 1960 conviction.

The Government also alleged that Binance's motive for avoiding the registration requirement was to prevent U.S. regulators from discovering that Binance was not maintaining an AML/KYC program and was, consequently, allowing its exchange to be used by a variety of "illicit actors," including: "mixing services" that laundered criminally derived cryptocurrency; persons moving the proceeds of ransomware; and persons moving the proceeds of "darknet market transactions."

For example, Binance facilitated $273 million in deposits and withdrawals from BestMixer, "one of the largest cryptocurrency mixers in the world," and $106 million in bitcoin transfers from Hydra, a "popular Russian darknet marketplace frequently utilized by criminals."

While facilitating thousands of such transactions, Binance never filed a single Suspicious Activity Report (SAR) with FinCEN. The failure to maintain an AML/KYC program and to file SARs was the basis for the Section 5318(h) conviction.

Finally, the Government alleged that Binance violated IEEPA by knowingly allowing its U.S.-based customers to use its platform to conduct transactions with persons and entities in sanctioned countries, including over $898 million in transactions with Iran.

Binance admitted to all of these allegations in its Plea Agreement, and its owner, Chengpeng Zhao, pled guilty to similar charges in a separate case. Sentencing is set for January 2024. *SDC*

Contact: AUSA Michael Dion and MLARS Attorney Kevin Mosley

Comment: This is obviously a major win for the Justice Department in its effort to crack down on those who facilitate money laundering through the cryptocurrency industry. Foreign-based cryptocurrency exchanges that have a significant customer base in the United States must register with FinCEN, and they must maintain effective AML/KYC programs. Binance did neither and is paying a heavy price.

A large part of that price is the $2.5 billion forfeiture money judgment. (As is all too typical, the mainstream press has referred to this as a "fine," reserving the term "forfeiture" for the kinds of cases the press likes to criticize; but that is an issue for another day.)

The legal basis for the forfeiture, however, is rather odd. The Information sets forth three grounds. First, it says that Binance must forfeit the "proceeds" of the Section 1960 offense pursuant to 18 U.S.C. § 981(a)(1)(C). Section 1960 is an SUA, so the forfeiture of the proceeds of the offense – presumably the fees earned by the company – would be authorized by § 981(a)(1)(C); but for whatever reason, the Plea Agreement does not base any part of the forfeiture on that ground.

Second, the Information says that Binance must forfeit all property "involved in" the Section 1960 violation pursuant to § 981(a)(1)(A). Forfeiture under that statute for an offense committed by a money transmitting business includes a sum of money equal to the total of all transactions conducted by the business while it was acting illegally. *See United States v. Elfgeeh,* 515 F.3d 100, 139 (2d Cir. 2008), and other cases cited in Section III.B of the Money Laundering Forfeiture Case Outline

Thus, the Government could have sought to have Binance forfeit an amount of money equal to the billions of dollars in transactions it had conducted in the six-year period in which it operated illegally. But instead, it opted to limit the forfeiture under § 981(a)(1)(A) to the $1.6 billion in fees that it earned from conducting those transactions – or in other words, to the "proceeds" that it could have forfeited under § 981(a)(1)(C) but did not.

Finally, the forfeiture amount included the $898 million transferred to Iran on the ground it was forfeitable under § 981(a)(1)(C) as the "proceeds" of the IEEPA offenses. In seeking to forfeit that amount from Binance, which obviously did not retain any of the money other than its fee, the Department seems to have set aside its view that the Supreme Court's decision in *Honeycutt* applies to § 981(a)(1)(C), and that accordingly forfeitures under that statute are limited to property that the defendant personally obtained.

The courts have split on that question, but the Government has conceded that forfeitures under § 981(a)(1)(C) are limited in that regard in several cases. *Compare United States v. Sexton,* 894 F.3d 787, 798-99 (6th Cir. 2018) (the "linchpin" of the *Honeycutt* decision was the phrase "proceeds the person obtained;" because § 981(a)(1)(C) contains no such limitation, *Honeycutt* does not apply) *with United States v. McIntosh,* 2023 WL 382945 (2nd Cir. Jan. 25, 2023) (unpub.) (Government concedes that *Honeycutt* applies to forfeitures under § 981(a)(1)(C) and that Defendant therefore cannot be jointly and severally liable for proceeds of Hobbs Act robbery). For whatever reason, in this case the Government took a different view.
The criminal information and the plea agreement are posted on my website at http://assetforfeiturelaw.us/?page_id=168. *SDC*

Reed

United States v. Reed, 2022 WL 597180 (S.D.N.Y. Feb. 28, 2022).

S.D.N.Y. * Defendant, the owner of a bitcoin exchange, was indicted for failing to have an adequate anti-money laundering program as required by 31 U.S.C. § 5318(h). He moved to dismiss the indictment on the ground that a bitcoin exchange is not required to have such a program; but the court denied the motion to dismiss.

Contact: AUSA Samuel Raymond

Commodity Futures Trading Comm'n

Commodity Futures Trading Comm'n, 2022 WL 1421479 (S.D.N.Y. May 5, 2022).

S.D.N.Y. * Defendant, the co-founder of a cryptocurrency trading platform known as BitMEX, pled guilty to causing a financial institution to violate 31 U.S.C. §§ 5318(h) and (l). In a separate action, the Commodity Futures Trading Commission sought an order restraining Defendant from engaging in cryptocurrency trading. The court, inter alia, found that Defendant failed to maintain an adequate anti-money laundering / Know Your Customer Program, entered the restraining order, and ordered Defendant to pay a $10 million civil money penalty.

Acquiring Illicit Goods with Crypto

Twenty-Four Cryptocurrency Accounts

Using the 'blockchain,' the Government identifies the accounts at a Bitcoin exchange that were used to pay for child pornography and brings a civil forfeiture action against those accounts.

The Government satisfies the notice requirement in Rule G(4) by sending notice by email to the email addresses of the account holders maintained by the Bitcoin exchanges.

A cryptocurrency account that has been used in the past to pay for child pornography is subject to forfeiture as property used to commit a child pornography offense.

United States v. Twenty-Four Cryptocurrency Accounts, 2020 WL 4049914 (D.D.C. July 20, 2020).

D.D.C. * Federal agents investigating a child pornography website determined that the website was based in South Korea, and using information obtained during a search by South Korean authorities, compiled a list of the website's customer accounts. The account information contained the unique Bitcoin addresses that each individual used to pay for downloaded pornographic material.

Using the "blockchain" and subpoena returns from Bitcoin exchanges, the agents were able to link the Bitcoin addresses used to pay for the downloaded material to Bitcoin "wallets" maintained in 24 accounts at three Bitcoin exchanges. The Government then filed a civil forfeiture complaint under 18 U.S.C. § 2254, alleging that the 24 accounts were property used to commit a child pornography offense under Section 2252.

To provide notice of the forfeiture action, the Government requested that each of the three Bitcoin exchanges provide the customer information that it was required to maintain under the applicable Know Your Customer regulations. The Government then sent a certified letter to each physical address and notice by email to any account holder who did not have a physical address. In this way, the Government reached 22 of the 24 account holders. It also posted notice of the forfeiture action on the Government's internet website.

When no one filed a claim, the Government moved for a default judgment. The principal question before the court was whether the method the Government used to send notice satisfied Rule G(4). The court held that it did.

The court noted that not every potential claimant had a valid physical address (some had no such address and the notice sent to others was returned undelivered). But in that case, the court said, sending notice by email was sufficient because it was valid to assume that persons using the internet to pay for child pornography with bitcoins have a level of internet proficiency. With respect to the account holders whose email address was no longer valid, the court said, the publication on www.forfeiture.gov was sufficient.

Finally, the court held that the bitcoin accounts that the account holders maintained at the Bitcoin exchanges, and that they had used in the past to pay for child pornography, were forfeitable as property used to commit a child pornography offense.

So, the court entered the default judgment as to all 24 accounts. *SDC*

Contact: AUSAs Zia Faruqui and Lindsay Suttenberg, and Trial Attorney Alden Pelker

Comment: This opinion is less than clear in explaining how the agents – from IRS and HSI – identified the defendant bitcoin accounts. The Government's civil forfeiture complaint does a much better job of that, so I have posted it on my website: www.assetforfeiturelaw.us.

The interesting question in this case was whether it is sufficient for purposes of Rule G(4) to send notice of the forfeiture of a bitcoin account maintained at a Bitcoin exchange to the email address that the account holder gave to the Bitcoin exchange when it opened the account. Whatever the sufficiency of sending notice by email might be in other situations, the court said, people who use bitcoins to make internet purchases may be assumed to have sufficient internet proficiency to make notice by email appropriate.

Finally, without discussing the matter, the court assumes that if a bitcoin account was used in the past to pay for child pornography, the current balance in that account is subject to forfeiture as property used to commit the child pornography offense. In other words, the court did not distinguish between the account itself and the cryptocurrency in the account the way courts might distinguish between a bank account that has been used in the past to commit a criminal offense and the balance in the account at a later date. *SDC*

Search of One Address

Evidence that a person has used cryptocurrency to purchase child pornography in the past is sufficient to establish probable cause to believe that he intends to use any cryptocurrency found in his possession to purchase child pornography in the future.

Cryptocurrency that a person intends to use to purchase child pornography is subject to seizure for forfeiture under Sections 2253 and 853(f).

In the Matter of the Search of One Address, 512 F.Supp.3d 23 (D.D.C. 2021).

D.D.C. * Homeland Security agents were investigating a marketplace on the "darknet" that distributed child pornography. They used cryptocurrency to make undercover purchases of pornographic material from the website and thereby, using blockchain analysis tools, were able to identify the cryptocurrency exchange that the website used to process sales.

The agents then subpoenaed the exchange to reveal the identity and location of a particular customer ("the Subject") who had used the exchange to purchase child pornography with bitcoins, and applied for a warrant authorizing the search of the Subject's premises and the seizure of all cryptocurrency and information (such as encryption keys) necessary to access such cryptocurrency that might be found there.

The court issued the warrant, emphasizing that the cryptocurrency and related information were subject to seizure not only as evidence, but pursuant to 21 U.S.C. § 853(f) and 18 U.S.C. § 2253, as property subject to forfeiture.

Section 2253 authorizes the forfeiture of any property used to commit or to promote the commission of a child pornography offense. The court noted that the bitcoins that had been used in the past to purchase child pornography would no longer be in the Subject's possession, but it held that the phrase "property intended to be used to promote" the commission of a child pornography offense would include all cryptocurrency found in the Subject's possession when the warrant was executed.

To justify the issuance of the seizure warrant under Section 853(f), the Government only had to show probable cause to believe that the property would be used in the future to commit a child pornography offense. "The (perceived) anonymity of cryptocurrency," the court said, "was crucial and necessary to the commission of the offense because it concealed the purchase of child pornography" in that it "allowed the Subject to operate without fear of discovery." Thus, cryptocurrency that a person intends to use to purchase child pornography falls within the scope of "property intended to be used to promote."

Moreover, given that the Subject had used cryptocurrency in the past to purchase child pornography, there was probable cause to believe that he intended to use the cryptocurrency remaining in his possession to do so again in the future.

So, the court authorized the seizure of any cryptocurrency found in any "wallet" that was in the Subject's possession. *SDC*

Contact: AUSAs April Russo and Janani Iyengar

Comment: This opinion contains strong language explaining how the use of cryptocurrency and the anonymity that it is perceived to provide facilitates the commission of a child pornography offense. Its more far-reaching holding, however, is that once a person is found to have used cryptocurrency such as bitcoins to purchase child pornography, there is probable cause to believe that *any* cryptocurrency found in his possession is forfeitable as property used or intended to be used to facilitate the offense. There is no need to trace or divide such funds, as the very nature of the medium was what facilitated the crime.

As the court points out, this contrasts with how courts treat cash: The fact that a person has used cash in the past to buy drugs, for example, does not by itself establish

probable cause to believe that any cash found in his possession will be used to buy drugs in the future. But the court holds that given the particular advantages of using cryptocurrency to purchase child pornography, the possession of such property by a person who has used cryptocurrency in the past to purchase child pornography is enough to establish probable cause to believe he will used it in the future for that purpose. *SDC*

Silk Road Cases

To survive a motion to dismiss for lack of standing, the claimant must allege facts that plausibly support his claim that his property is included in the property subject to forfeiture.

A claimant's speculation – or conclusory assertion – that property stolen from him must be included in the defendant property is insufficient.

United States v. Approximately 69,370 Bitcoin, 2022 WL 888655 (N.D. Cal. Mar. 25, 2022).

N.D. Cal. * The Silk Road was an online marketplace that served as a "black market bazaar" where unlawful goods and services were bought and sold, exclusively in exchange for Bitcoin. Before it was shut down by law enforcement in 2013, someone hacked into Silk Road and stole $14 million in Bitcoin.

Years later, IRS agents determined who the thief was, tracked the Bitcoin (now worth $3.5 billion) to a cryptocurrency wallet, and obtained the thief's consent to its forfeiture.

In the ensuing civil forfeiture action, multiple persons filed claims asserting that all or part of the subject Bitcoin belonged to them. The Government moved to strike each claim for lack of standing.

For example, Claimant One asserted that a quantity of Bitcoin had been stolen from his wallet at a Bitcoin exchange called Mt. Gox and speculated that the thief had transferred the money to the Silk Road where it was stolen again and included in the Bitcoin that the Government had recovered. The court held, however, that Claimant One had "not pointed to a single fact" supporting his claim. To the contrary, the court said, he had "done nothing more than show that he owned some Bitcoin that was stolen from him, and then baldly claimed that [some of the Bitcoin stolen from Silk Road] must be his."

Claimant Two asserted that he had a quantity of Bitcoin in his Silk Road account at the time the website was shut down, but that because Bitcoin is fungible, he was entitled to make a claim to the Bitcoin that had been stolen earlier and then recovered.

The court held, however, that this was tantamount to a claim that Claimant Two's Bitcoin was simultaneously in his Silk Road account and included in the Bitcoin stolen by the hacker. Such a claim, the court said, is insufficient to establish standing.

Finally, Claimant Three was an investor that had purchased the assets of a bankruptcy estate. It alleged in conclusory fashion without any supporting evidence that all $3.5 billion of the stolen Bitcoin was included in the estate. But the court held that Claimant Three had not alleged any facts that plausibly supported such a claim.

So, the court granted all of the Government's motions to dismiss. *SDC*

Contact: AUSA David Countryman

Silk Road Cases

To survive a motion to dismiss for lack of standing, the claimant must allege facts that plausibly support his claim that he has an interest in the property subject to forfeiture.

A claimant's speculation – or conclusory assertion – that property stolen from him must be included in the defendant property is insufficient.

A person who acquires property after learning that it is subject to forfeiture cannot be an innocent owner.

United States v. Approximately 69,370 Bitcoin, 2022 WL 2755353 (N.D. Cal. July 14, 2022).

N.D. Cal. * The Silk Road was an online marketplace that served as a "black market bazaar" where unlawful goods and services were bought and sold, exclusively in exchange for bitcoin. Before it was shut down by law enforcement in 2013, someone hacked into Silk Road and stole $14 million in bitcoin.

Years later, IRS agents determined who the thief was, tracked the bitcoin to a cryptocurrency wallet, seized it, and obtained the thief's consent to its forfeiture.

In the ensuing civil forfeiture action, multiple persons filed claims asserting that all or part of the seized bitcoin belonged to them. The Government moved to strike each claim for lack of standing and the court granted the motion as to most of the claims, leaving one claim unresolved. *United States v. Approximately 69,370 Bitcoin*, 2022 WL 888655 (N.D. Cal. Mar. 25, 2022).

In the remaining case, Claimant asserted that he had purchased a fractional bitcoin after the defendant property was seized and named in the forfeiture action. Even if Claimant's assertion that the bitcoin he purchased was part of the seized bitcoin was correct, the court said, Claimant could not be an innocent owner, as 18 U.S.C. § 983(d)(3) requires a showing that the claimant "did not know and was reasonably without cause to believe that the property was subject to forfeiture" at the time he acquired his interest in it. Because Claimant alleged that he purchased the bitcoin after It was named in the forfeiture complaint, he could not qualify.

But the claim would fail in any event, the court said, because Claimant "offers nothing more than undue speculation that any of the seized bitcoin is his property."

To withstand a motion to strike his claim at the pleading stage, Claimant had to allege facts showing that the bitcoin that he purchased was part of the seized property. "Conclusory and/or implausible assertions" are not enough.

Because Claimant "offered nothing other than guesses and bald assertions in support of his contention" that the bitcoin that he purchased somehow ended up in the wallet that was seized, his claim did not meet the pleading standard.

So, the court granted the Government's motion to strike the claim. *SDC*

Contact: AUSA David Countryman

Adegboruwa

That a person agreed to use cryptocurrency to purchase drugs from a drug organization is not sufficient, by itself, to show that the person joined the drug traffickers' conspiracy to commit money laundering.

United States v. Adegboruwa, 2023 WL 4491531 (D. Utah Jul. 12, 2023).

D. Utah * Defendant, facing trial on drug and money laundering conspiracy charges, moved to exclude certain third party statements as inadmissible hearsay. The Government opposed the motion, arguing that the statements were admissible under F.R.Evid. 801(d)(2)(E) as statements made in furtherance of a money laundering conspiracy by co-conspirators.

The statements in question were made by customers of Defendant's drug organization who agreed to use cryptocurrency to pay for the drugs that they were

purchasing. But the court held that the customers' agreement to use cryptocurrency to make their purchases did not mean that they were members of Defendant's money laundering conspiracy.

"Frankly," the court said, "the individuals who purchased illicit narcotics from the distribution conspiracy did not care what happened to the money they spent once it was out of their pockets." Accordingly, the court concluded, there was no evidence that the purchasers intended to join a conspiracy to launder the drug proceeds, and thus their statements were not admissible as co-conspirator statements under the exception to the hearsay rule. *SDC*

Contact: AUSA Cy Castle

Using Crypto to Commit New Crimes in New Ways

Approximately 3879.16242937 bitcoin

Entering a default judgment as to all potential claimants who did not file claims allows the Government to enter into a settlement with the claimant who did file a claim without fear that another third party would be able to object to the settlement.

When a civil forfeiture action is brought against cryptocurrency, the Government may sell the cryptocurrency in an interlocutory sale, making the proceeds a "substitute res."

United States v. Approximately 3879.16242937 bitcoin, 2022 WL 2128908 (S.D. Cal. Apr. 18, 2022).

S.D. Cal. * Defendant, the employee of an insurance company, stole $154,982,103 from his employer by directing the employer's bank in Bermuda to wire that amount to Defendant's bank account in California. Defendant then used the money to purchase approximately 3,879.16 bitcoin.

The Government filed a civil forfeiture action against the bitcoin in which only one Claimant – the employer's reinsurer – filed a claim. The Government then sold the bitcoin in an interlocutory sale (yielding $161,660,054, which became the "substitute *res*") and moved for a default judgment as to Defendant and any other third party who had not filed a claim.

The Government explained that it was requesting the partial default judgment to allow it to enter into a settlement agreement with Claimant, recognizing its interest in the substitute *res*, "without fear that any other claimant may one day assert a belated claim to the property."

The court accepted the Government's explanation, found that there was a factual basis for the forfeiture, and entered a judgment in favor of the Government as to all third parties other than Claimant. *SDC*

Contact: AUSA Aaron Arnzen

Comment: While not a common occurrence, the entry of a default judgment as to "everyone but the claimant" is a useful device for ensuring that the Government can enter into a settlement with the claimant without having to worry that another third party will come forward and object that the Government had no right to surrender his property to the claimant. *SDC*

Approximately 3879.16242937 bitcoin
Embezzler commits a concealment money laundering offense when he diverts his employer's funds to a Coinbase account, and then instructs Coinbase to convert the money to bitcoin.

The victim of an embezzlement retains ownership of the embezzled funds, and is entitled to the return of the appreciated value of the bitcoin when they are converted back to dollars.

United States v. Approximately 3879.16242937 bitcoin, 2022 WL 11625551 (S.D. Cal. Jul. 12, 2022).

S.D. Cal. * The employee of a Japanese insurance company embezzled $155 million from his employer by diverting the money from the employer's account at a foreign bank to a bank account in California. The California account was a Coinbase account that the employee falsely represented to be controlled by his employer.

The employee then laundered the money in the Coinbase account by instructing Coinbase to convert the $155 million to bitcoin in a wallet that he controlled.

With the assistance of Japanese law enforcement, the FBI seized the bitcoin by transferring it to the FBI's bitcoin wallet. The Government then filed a civil forfeiture action against the bitcoin, alleging *inter alia* that it was property involved in a concealment money laundering offense, and moved for an interlocutory sale so that it could be converted back to dollars. The court granted the motion, designating the $161 million in proceeds as a substitute *res.*

The employer-victim filed the only claim, and the Government agreed to recognize the claim in a settlement agreement, returning all $161 million to the victim of the embezzlement. *SDC*

Contact: AUSA Aaron Arnzen

Comment: There is no legal issue in this case, but it illustrates how cryptocurrency is used to launder criminal proceeds, and how the Government handles the seizure of cryptocurrency and its conversion back to fiat currency.

First, the embezzler deposited his employer's money into a bank account associated with Coinbase, doing so by falsely representing that the account belonged to his employer. He then laundered the money by instructing Coinbase to convert the money to bitcoin and to transfer it to a wallet that the embezzler controlled.

When the scheme was discovered, the FBI seized the bitcoin by transferring it to the FBI's bitcoin account, and the Government converted it back to dollars via a motion for an interlocutory sale, with the proceeds of the sale becoming a substitute *res.*

Two things about the money laundering offense are also worth noting: For purposes of the money laundering statute, the embezzled money became SUA proceeds at the time it was placed in the Coinbase account, even though the scheme was not yet complete, because it was the proceeds of the first phase of the embezzlement scheme and had come under the embezzler's control. And the subsequent conversion of the proceeds to bitcoin in the embezzler's wallet was considered evidence that the transaction was conducted to conceal or disguise those proceeds.

Finally, note that the victim of an embezzlement has standing to object to the forfeiture of the embezzled funds because -- unlike the victim of, say, an investment fraud scheme – it did not voluntarily surrender title to its property and thereby become an unsecured creditor. *See United States v. Emor,* 785 F.3d 671 (D.C. Cir. 2015) (fraud victims may lack standing as unsecured creditors, but if the claimant is able to show that it was the victim of embezzlement, it could prevail in the ancillary proceeding under § 853(n)(6)(A)).

Accordingly, the victim was entitled to the return of all of the embezzled funds – or in this case – the substitute *res* which increased in value by more than $6 million in the process of converting it back from bitcoin to fiat currency. *SDC*

Approximately 32,113.63 Tether

Court declines to grant a default judgment where the Government's civil forfeiture complaint does not explain why the Government is entitled to forfeit all funds seized from a cryptocurrency account, instead of only the portion traceable to the alleged fraud.

But the court gives the Government leave to amend its complaint to explain how cryptocurrency commingled with the fraud proceeds might be forfeitable under a money laundering theory.

United States v. Approximately 32113.63 Tether (USDT) Cryptocurrency, 2023 WL 1108729 (E.D. Wis. Jan. 30, 2023).

E.D. Wis. * The Government filed a civil forfeiture complaint against a quantity of cryptocurrency seized from an account at Binance in California, alleging that it was the proceeds of a wire fraud scheme and property involved in money laundering.

According to the complaint, the victim of a fraud scheme received a phone call from a person representing himself to be a commissioner with the Federal Trade Commission (FTC), and advising him that his identity had been stolen and that he needed to purchase $15,000 in bitcoin and transfer it to the FTC to resolve the matter. The victim did as he was instructed and sent the bitcoin to a specific bitcoin address. When he realized that this might be a fraud scheme, he contacted law enforcement.

The complaint also described what happened to the victim's bitcoin once it arrived in the bogus FTC account. Law enforcement was able to establish through blockchain analysis that it was commingled with additional bitcoin from other sources, and that it was included in the transfer of approximately $40,000 in bitcoin to an account at Binance, where it was converted to the defendant 32,113.63 Tether (USDT) – another type of cryptocurrency. The Government then seized the entire 32,113.63 Tether (USDT) and filed the instant civil forfeiture complaint against it.

The Government sent notice of the forfeiture action against the seized assets to the person in India registered with Binance as the owner of the account, but no claim was filed. Accordingly, the Government moved for a default judgment against the seized funds.

The court found that the notice to the account holder in India was sufficient to satisfy due process, but nevertheless denied the motion for a default judgment.

According to the complaint, the court said, only $15,000 of the victim's money was traceable to the 32,113.63 Tether (USDT) seized from the Binance account. The remainder represented commingled funds. "Because the allegations in the complaint do not support a judgment in the amount of 32,133.63 Tether (USDT)," the court said, "the court must deny the motion for a default judgment."

Nevertheless, the court said that it would permit the Government to amend its complaint to demonstrate why it was entitled to the forfeiture of the full amount. *SDC*

Contact: AUSA Bridget Schoenborn

Comment: When the Government seeks the forfeiture of funds from an account under a proceeds theory, it is limited to the portion of the funds that are traceable to the crime that generated the proceeds. (It is the same whether the account is a traditional bank account or a cryptocurrency account held by a crypto exchange like Binance.)

Here, the crime that generated the proceeds was the wire fraud perpetrated against the victim who was induced to send $15,000 worth of bitcoin to a bitcoin account. So, under a proceeds theory, the Government would be entitled only to forfeit the portion of the funds in the Binance account where the funds ended up that were traceable to the victim's $15,000.

Accordingly, it was reasonable for the court to ask, what is the justification for seizing and forfeiting cryptocurrency worth nearly $40,000?

The answer is that the Government's complaint did not rely only on a proceeds theory but also alleged that the seized cryptocurrency was involved in a money laundering offense. Presumably, the money laundering offense occurred when the perpetrators of the fraud commingled the bitcoin received from the victim with bitcoin from other sources, and transferred the combined amount to the Binance account.

It is well-established that the forfeiture of property "involved in money laundering" offenses is not limited to the criminal proceeds being laundered but includes any commingled assets that were part of the alleged money laundering transaction. *See* Section II.B.2 of the Money Laundering Forfeiture Case Outline and Chapter 27 of *Asset Forfeiture Law in the United States* (3d ed. 2022) (discussing the scope of the term "property involved in money laundering").

Here, if the $15,000 in bitcoin taken from the victim was commingled with nearly $25,000 in bitcoin from other sources and transferred in violation of the money laundering laws to the Binance account, the entire sum would be subject to forfeiture as property involved in the money laundering offense.

Presumably, the Government will amend its civil forfeiture complaint to make this clear. *SDC*

Approximately 32113.63 Tether

When fraud proceeds and funds from an unknown source are deposited into an account at about the same time, and in similar circumstances, there is reasonable grounds to believe that all of the funds are fraud proceeds.

United States v. Approximately 32113.63 Tether (USDT) Cryptocurrency, 2023 WL 1108729 (E.D. Wis. Aug. 18, 2023).

E.D. Wis. * The Government filed a civil forfeiture complaint against a quantity of cryptocurrency seized from an account at Binance in California, alleging that it was the proceeds of a wire fraud scheme and property involved in money laundering.

According to the complaint, the victim of a fraud scheme sent $15,000 in bitcoin to a specific bitcoin address, where it was commingled with additional bitcoin from other sources and then transferred to an account at Binance, where it was converted to the defendant 32,113.63 Tether (USDT) – another type of cryptocurrency. The Government then seized the entire 32,113.63 Tether (USDT) and filed the instant civil forfeiture complaint against it.

When no one filed a claim, the Government moved for a default judgment against the seized funds, but the court held that because the complaint's proceeds theory only supported the forfeiture of a portion of the seized funds, the motion would be denied. *United States v. Approximately 32113.63 Tether (USDT) Cryptocurrency*, 2023 WL 1108729 (E.D. Wis. Jan. 30, 2023) (March 2023 *Digest*).

The Government then filed an amended complaint, alleging that given the timing and circumstances, there was reason to believe that all of the seized funds were traceable to fraud, or alternatively that the commingling of the funds constituted a money laundering offense.

The court agreed that the Government's timing and circumstances argument set forth sufficient grounds for recovery under the proceeds theory, and granted the motion for a default judgment on that basis without reaching the money laundering theory. *SDC*

Contact: AUSA Bridget Schoenborn

Comment: In my comment on this case in the March *Digest,* I noted that the Government did not rely solely on the proceeds theory in its original complaint but also alleged that the commingled funds were forfeitable as property involved in a money laundering offense. Because it is well-established that commingled funds are forfeitable

in their entirety in money laundering cases, I suggested that the court erred in failing to enter the default judgment.

When it filed its amended complaint, the Government explained the money laundering forfeiture theory in detail, but it also argued that when fraud proceeds are commingled with other funds that are deposited at about the same time and under similar circumstances, the evidence is sufficient to establish that all of the funds are forfeitable as proceeds. (For a discussion of the money laundering theory, see the Comment following the next case summary.)

The court accepted the proceeds theory and accordingly did not address the money laundering theory. *SDC*

Approximately 1.10387626 Bitcoin

Secret Service traces defrauded victim's cryptocurrency through the blockchain to a wallet at Binance, which froze the account and provided KYC information including the account holder's name and email address.

Notice by email is sufficient to satisfy the notice requirements under Rule G(4).

United States v. Approximately 1.10387626 Bitcoin, 2024 WL 490460 (E.D. Cal. Feb. 8, 2024).

E.D. Cal. * A person impersonating a Secret Service agent called Victim, told him that his bank account had been compromised, and said that to secure his funds, he should transfer the contents of the account to a "secured digital wallet." Victim complied, transferring $40,000 to a digital wallet using a QR code supplied by the caller.

Realizing that he had been defrauded, Victim contacted the Secret Service which traced his funds to a Binance account. At the Service's request, Binance froze the account and the Government ultimately seized the funds with a seizure warrant.

Using the information Binance maintained in its Know Your Customer (KYC) file, the Government sent notice by email to the Account Holder, who did not respond. So, the Government moved for, and the court entered, a default judgment. *SDC*

Contact: AUSA Kevin Khasigian

Comment: This case illustrates two things of particular interest: First, that a supposedly anonymous cryptocurrency transaction is not anonymous at all if the law enforcement agency can trace the cryptocurrency through the blockchain to a wallet maintained by a legitimate cryptocurrency exchange that, in turn, has a record of the account holder's name and contact information in its KYC file.

Second, to satisfy the notice requirement under Rule G(4) when it had nothing more than a name and an email address, the Government requested, and the court issued, an order directing that notice by email would satisfy the notice requirements in the circumstances of this case. *SDC*

Arcaro

Even in the Ninth Circuit, a fraud victim cannot recover his losses under a constructive trust theory unless he can trace his losses to the forfeited property.

United States v. Arcaro, 2024 WL 40213 (S.D. Cal. Jan. 3, 2024).

S.D. Cal. * Defendant operated a cryptocurrency trading platform called BitConnect as a global Ponzi scheme that defrauded investors of millions of dollars. He pled guilty to conspiracy to commit wire fraud and agreed to pay a forfeiture money judgment in the amount of $24 million as well as restitution to his victims. The court entered appropriate forfeiture and restitution orders.

To satisfy those orders, Defendant surrendered a quantity of bitcoin to the Government that, when liquidated, yielded nearly $39 million. The court applied $17 million of this amount to the restitution order and the remainder the forfeiture judgment, and then conducted an ancillary proceeding to determine if any third parties had valid claims to the forfeited amount. Ninety-seven claimants filed claims.

After a thorough discussion of the law governing the ancillary proceeding in a criminal forfeiture case – which, in the Ninth Circuit, provides that fraud victims are entitled to recover as the beneficiaries of a constructive trust if they can trace their losses to the forfeited property – the court addressed all 97 claims.

It dismissed 41 of the claims for failure to comply with the pleading requirements in 21 U.S.C. § 853(n)(3) in that they were not filed under penalty of perjury or failed to provide documentation supporting the claim. It dismissed another nine claims because the claimant had already recovered his losses through restitution, and 16 claims because the claimant could not trace his purported interest to the forfeited property.

Finally, the court granted the remaining claims because an FBI analyst was able to verify that each claimant could satisfy the tracing requirement. *SDC*

Contact: AUSA Carl Brooker

Comment: As a general matter, fraud victims lack standing to contest the forfeiture of the fraudsters assets because they are unsecured creditors with no legal interest in the forfeiture property. The remedy for such victims is to ask the Government to apply any forfeited property to satisfy a restitution order or to file a remission petition.

One exception to that rule applies when the victim can satisfy the elements of constructive trust under state law. In that case, the court may find that the claimant has a legal interest in the property that was superior to the defendant's (and the Government's) interest under 21 U.S.C. § 853(n)(6)(A). Recover under a constructive trust theory is rare, however: Claimants usually will not be able to satisfy all of the elements of a constructive trust, or the court will find that a constructive trust, as an equitable remedy, should not be imposed because doing so would be unfair to other victims who are unable to satisfy the constructive trust requirements. All of this is discussed in detail in Section 23-15(g) of *Asset Forfeiture Law in the United States* (3d ed. 2022), and the cases are collected in Section XX.H of the Criminal Forfeiture Case Outline.

The Ninth Circuit takes a more liberal view of what interest must be asserted to establish a valid constructive trust claim than any other circuit. *See United States v. $4,224,958.57,* 392 F.3d 1002, 1005 (9th Cir. 2004) (*Boylan*) (all fraud victims have standing to contest the forfeiture of the fraudster's property as potential beneficiaries of a constructive trust and are entitled to notice of the forfeiture proceeding); *United States v. Wilson*, 659 F.3d 947, 956 (9th Cir. 2011) (holding that once a given victim is able to trace, and the constructive trust is created, the court is entitled to ignore the tracing requirement and administer the trust as in a liquidation proceeding for the benefit of all victims). Nevertheless, as the court in this case holds, the claimant still must satisfy the tracing requirement.

The bottom line is that some of the victims in this case were able to satisfy the relaxed requirements that prevail in the Ninth Circuit but others were not. *SDC*

Approximately 1,360,000.748 Tether

FBI traces fraud victim's cryptocurrency investment through multiple crypto addresses using blockchain analysis, and recovers millions in funds through civil forfeiture.

United States v. Approximately 1,360,000.748 Tether, 2024 WL 348815 (N.D. Cal. Jan. 30, 2024).

N.D. Cal. * A person believed to be a Chinese national, but who was otherwise unknown, befriended Victim through social media and told her of his great success in investing in cryptocurrency. At the unknown person's direction, Victim downloaded an investment app called NYMEX, purchased over a million dollars in stable coins on legitimate cryptocurrency exchanges such as Coinbase, and transferred them to the NYMEX website to invest. When the website indicated that Victim was enjoying huge gains, she convinced family members to add their funds to the NYMEX investment.

Altogether, Victim and her family transferred $5.5 million in stable coins to the website, only to discover, when they were unable to withdraw their funds, that the website was a fraud, and that all of the purported "gains" were fictitious.

The FBI was able to use blockchain analysis to trace Victim's money through a series of transfers between cryptocurrency addresses called "hops" where the funds were converted to other cryptocurrencies such as DAI, USDC and Tether, before coming to rest in a particular account. Moreover, the investigation revealed that along the way, Victim's funds had been combined with millions of dollars in cryptocurrencies from at least 29 other persons who complained that they were also victims of a similar investment fraud.

The Government obtained a seizure warrant for the account and commenced a civil forfeiture action alleging that the funds constituted property involved in money laundering. It sent notice to the address of the Chinese national who appeared to be associated with the account, but when no one filed a claim, it moved for a default judgment.

Finding that the Government had complied with all procedural requirements in Rule G, the court granted the motion. *SDC*

Contact: AUSA Galen Phillips

Comment: While this default judgment does not make any new law, it nevertheless illustrates how blockchain analysis can allow law enforcement to trace a victim's money through numerous conversions – involving numerous cryptocurrency addresses – to a given location and then recover the money with a seizure warrant, even though the perpetrators of the underlying fraud are unknown.

It also illustrates two other points: That funds commingled with the victim's funds in the course of the "hops" through the cryptocurrency addresses are forfeitable as property involved in the money laundering offense, whether or not those funds can be traced to a particular fraud victim; and that civil forfeiture is the essential tool for recovering such funds where the perpetrator of the fraud is unknown and, in all events, is likely located beyond the jurisdiction of the U.S. courts. *SDC*

Theft of Cryptocurrency

Search of Multiple Email Accounts

Software used to analyze the blockchain and connect cryptocurrency transactions to each other and to individuals and their assets is sufficiently reliable to serve as the probable cause for the issuance of a search warrant.

Venue for a money laundering conspiracy lies in any district where an overt act in furtherance of the SUA that is the object of the conspiracy took place.

In the Matter of the Search of Multiple Email Accounts, 585 F.Supp.3d 1 (D.D.C. 2022).

D.D.C. * Defendants were arrested and charged with conspiring to launder 119,754 Bitcoins stolen from a Hong Kong-based virtual currency exchange. Bitcoins valued at $3.6 billion were seized at the time of the arrest.

In the course of the investigation leading to the arrests and seizure, federal agents applied for a warrant to search Defendants' email accounts, presumably to establish Defendants' connection to the offense and to locate the virtual currency. The magistrate judge issued the warrant accompanied by a detailed opinion setting forth the probable cause. The opinion remained sealed until the arrests and seizure took place.

As a threshold matter, the court had to determine whether Washington, DC was the appropriate venue for issuing the warrant. Under the Federal Rules of Criminal Procedure, a warrant to search for evidence in a money laundering case may be issued in any district where there is probable cause to believe the money laundering offense took place. The Government's affidavit alleged that in laundering the stolen Bitcoins, Defendants had committed an international promotional money laundering offense with the intent to promote a violation of the bank fraud statute, 18 U.S.C. § 1344. So, the question was whether there was probable cause to believe that that money laundering offense occurred at least in part in the District of Columbia.

The court held that there was probable cause to believe that Defendants committed bank fraud when they converted some of the stolen Bitcoins to deposits at traditional financial institutions without informing the institutions of the true source of the

money, and that they engaged in international money laundering when they arranged international transfers in furtherance of that offense. Neither the financial institutions nor Defendants were in Washington, DC, and none of the international transfers involved in the money laundering offense occurred in that district, but the court held that that made no difference.

This misstatements to the banks, the court said, deprived them of their ability to detect the money laundering activity and to file Suspicious Activity Reports with FinCEN, which is located in Washington, DC. Thus, the bank fraud occurred at least in part in the District of Columbia, and because the bank fraud was an overt act in furtherance of the money laundering conspiracy, there was venue for the conspiracy in the District of Columbia.

The court then turned to the probable cause for the warrants. The Government's evidence was based on an analysis of the blockchain that was undertaken using commercially available software that detects "clusters" of seemingly unrelated transactions and links them together. The court first held that using such "clustering tools" to analyze the blockchain does not itself require a warrant because the blockchain is publicly accessible, and that using the results of the blockchain analysis to establish probable cause is appropriate because the analysis is highly reliable.

Accordingly, the court held that there was probable cause to issue the warrants for Defendants' email accounts. *SDC*

Contact: AUSA Chris Brown

Comment: The court does a masterful job of connecting the dots necessary to establish venue for issuing the search warrants in the District of Columbia. Among other things, it holds that there is venue for a money laundering conspiracy in any district where an overt act in furtherance of *the SUA* that is the object of the conspiracy takes place, that providing misinformation to a bank regarding the nature of a transaction is a bank fraud offense that occurs in part in Washington, DC because it "trick[s] the institution into not filing a SAR;" and that accordingly, there is venue in the District of Columbia for any money laundering conspiracy that involves such a violation of the bank fraud statute.

On the substance, this is the first case to hold that evidence obtained from blockchain analysis is sufficiently reliable to constitute probable cause regarding the connection between stolen or illegally-derived cryptocurrency on one hand, and the perpetrators of the offense and their subsequently-acquired assets on the other. *SDC*

Seizure of ICX Tokens

Property that was seized for forfeiture under federal law, but which later is named in a state civil forfeiture action, may remain in federal custody at the request of the state court, even though federal authorities, in deference to the State, have not filed a forfeiture action.

Under the abstention doctrine, court declines to exercise jurisdiction over a Rule 41(g) motion for the return of seized property, even though there is no pending federal forfeiture action, where doing so would interfere with a pending state forfeiture action.

In Re: Government Seizure of ICX Tokens, 2022 WL 292923 (D. Col. Jan. 31, 2022).

D. Col. * Claimant took advantage of a software bug in a user-controlled crypto-currency network and transferred millions of dollars in crypto assets to himself. Deeming this to have been a theft of property, the FBI obtained a warrant to seize the assets and commenced an administrative forfeiture action against them.

Claimant filed a claim but before the Government commenced a judicial forfeiture action, the State of Colorado indicted Claimant and filed its own civil forfeiture action against the assets. The state also obtained a TRO directing the FBI to maintain custody of the assets on the State's behalf pending the resolution of the criminal and civil cases.

Accordingly, the Government advised the court that it would not file a forfeiture action, but the FBI continued to maintain custody of the property pursuant to the State TRO.

Claimant filed a Rule 41(g) motion, arguing that once the federal authorities decided not to pursue a federal forfeiture action, they were obligated to return his property to him. But the court held that in light of the state civil forfeiture action and TRO, it would invoke the abstention doctrine of *Younger v. Harris,* and decline to exercise jurisdiction over Claimant's motion.

State courts in Colorado, the court said, provide Claimant with an adequate forum for relief from the state TRO. So, there was no reason for the federal court to interfere.

Accordingly, Claimant's Rule 41(g) motion was denied. *SDC*

Contact: AUSA Tonya Andrews

Silk Road Cases

To survive a motion for summary judgment for lack of standing, the claimant must allege facts that plausibly support his claim that his property is included among the assets subject to forfeiture.

A claimant's speculation – or conclusory assertion – that property stolen from him was part of the defendant property is insufficient.

Claimant is not automatically entitled to conduct discovery to establish his standing before the Government moves for summary judgment.

Person who knew he was acquiring property subject to forfeiture cannot be an innocent owner under § 983(d)(3).

United States v. Battle Born Investments, 2023 WL 5319258 (9th Cir. Aug. 18, 2023) (unpub.); *United States v. Hossain*, 2023 WL 5319262 (9th Cir. Aug. 18, 2023) (unpub.); *United States v. Buckley*, 2023 WL 5319260 (9th Cir. Aug. 18, 2023) (unpub.).

Ninth Circuit * The Silk Road was an online marketplace that served as a "black market bazaar" where unlawful goods and services were bought and sold, exclusively in exchange for Bitcoin. Before it was shut down by law enforcement in 2013, someone hacked into Silk Road and stole $14 million in Bitcoin.

Years later, IRS agents determined who the thief was, tracked the Bitcoin (now worth $3.5 billion) to a cryptocurrency wallet, and obtained the thief's consent to its forfeiture.

In the ensuing civil forfeiture action, multiple persons filed claims asserting that all or part of the subject Bitcoin belonged to them. The Government moved to strike each claim for lack of standing.

For example, Claimant One asserted that a quantity of Bitcoin had been stolen from his wallet at a Bitcoin exchange called Mt. Gox and speculated that the thief had transferred the money to the Silk Road where it was stolen again and included in the Bitcoin that the Government had recovered. Claimant Two asserted that he had a quantity of Bitcoin in his Silk Road account at the time the website was shut down, but that because Bitcoin is fungible, he was entitled to make a claim to the Bitcoin that had been stolen earlier and then recovered. And Claimant Three was an investor that had purchased the assets of a bankruptcy estate. It alleged in conclusory fashion without any supporting evidence that all $3.5 billion of the stolen Bitcoin was included in the estate.

The district court held that none of the claimants had provided sufficient evidence to establish standing and granted all of the Government's motions to dismiss. *United*

States v. Approximately 69,370 Bitcoin, 2022 WL 888655 (N.D. Cal. Mar. 25, 2022) (May 2022 *Digest*). All three Claimants appealed.

In three separate unpublished opinions, the Ninth Circuit affirmed the district court.

In each case the panel held that while Claimants' "unequivocal assertion of ownership" of the defendant property was sufficient to establish standing at the pleading stage, it was not sufficient to overcome the Government's motion to dismiss under Rule G(8)(c) at the summary judgment stage. Rather, to defeat summary judgment for lack of standing, Claimants must "present some evidence of ownership beyond the mere assertion" of it, "and a conclusory, self-serving affidavit, lacking detailed facts and any supporting evidence, is insufficient" to do so.

Because none of the claimants supported their claims of ownership with anything "beyond mere speculation," the court said, none of them had provided enough evidence to create a material issue of fact sufficient to overcome a motion for summary judgment for lack of standing.

Moreover, the panel affirmed the district court's refusal to allow Claimants to conduct discovery on the standing issue under Rule 56 before granting summary judgment. "Nothing in Rule G(8)," the court said, "precludes the Government from moving to strike a claim prior to discovery."

Finally, with respect to one of the claims (*Buckley*), the court affirmed the district court's entry of summary judgment for an additional reason.

In that case, Claimant acknowledged that he had purchased his interest in the defendant bitcoin on the day he filed his claim – *i.e.,* after the Government filed its civil forfeiture complaint. He asserted that he was nevertheless a bona fide purchaser for value within the meaning of 18 U.S.C. § 983(d)(3) because the bitcoin was not "subject to forfeiture" until the court entered a forfeiture judgment. But the panel held that Claimant's knowledge of the pending forfeiture action at the time he acquired his alleged interest was sufficient to defeat his innocent owner claim.

So, the entry of summary judgment as to all three Claimants was affirmed. *SDC*

Contact: AUSA David Countryman (N.D. Cal.)

Comment: The voluminous and complicated case law discussing the standards for establishing standing at the various stages of a civil forfeiture case are collected in Section XIII.D. of the Civil Forfeiture Case Outline, and are discussed in detail in Chapter 9 of *Asset Forfeiture Law in the United States* (3d ed. 2022). *SDC*

113 Virtual Currency Accounts

A federal court has jurisdiction to order the forfeiture of funds in a foreign country that were involved in money laundering offenses that occurred at least in part in the United States.

Transferring stolen virtual currency through "peel chain" transactions constitutes concealment money laundering.

Transferring stolen virtual currency to co-conspirators, and using it to pay for infrastructure needed to keep the scheme going constitutes promotional money laundering.

Using stolen cryptocurrency to run an unlicensed money transmitting business is also promotional money laundering because a violation of Section 1960 is a "specified unlawful activity."

All property involved in a money laundering transaction is subject to forfeiture, including commingled funds from other sources.

United States v. 113 Virtual Currency Accounts, 2024 WL 940141 (D.D.C. Mar. 5, 2024).

D.D.C. * Defendants, operatives acting on behalf of North Korea, posed as potential customers of virtual currency exchanges in the United States and elsewhere. By inducing the managers of the exchanges to download malware onto their systems, Defendants gained access to the exchanges' customers' private keys, enabling them to steal hundreds of millions of dollars in virtual currencies. One exchange reported the loss of $250 million; others reported losses of $30 million and $48.5 million, respectively.

Defendants transferred the stolen currencies through a series of "peel chain" transactions whereby a fraction of the stolen money was "peeled off" at each step, and placed in another account. Along the way, some of the money was used to run a money transmitting business in which Defendants would exchange virtual currency for fiat currency for a fee. Ultimately, however, most of the stolen money was deposited into 145 virtual currency accounts in China held by co-conspirators. According to the Government, all of this was part of a scheme to use the stolen assets to fund North Korea's nuclear weapons program.

Defendants were indicted for money laundering and for running an unlicensed money transmitting business but remain outside the jurisdiction of the United States. So, the Government filed a civil forfeiture complaint against the 145 accounts, alleging that the funds in those accounts were subject to forfeiture under 18 U.S.C. § 981(a)(1)(A) as property involved in a conspiracy to commit concealment and promotional money laundering and to operate an unlicensed money transmitting business. When no one filed a claim, the Government moved for a default judgment.

As a threshold matter, the court held that the Government's efforts to send notice of the forfeiture action by email to the addresses associated with the virtual currency transactions satisfied the notice requirements in Rule G(4), and that the court had jurisdiction to issue an order against foreign assets because at least some transactions in the conspiracy involved exchanges in the United States.

The court also held that the complaint alleged violations of the money laundering laws: The theft of the funds from the virtual currency exchanges constituted wire fraud, which meant that the funds were the proceeds of a specified unlawful activity (SUA); the transmission of the funds through the "peel chain layering process" constituted concealment money laundering because it concealed the source of the funds; and distributing the wire fraud proceeds to conspirators in China constituted promotional money laundering.

In addition, the court said, Defendants committed promotional money laundering in two other ways: when they used the stolen funds to pay for domain registration, site hosting, and other infrastructure needed to perpetrate the scheme; and when they used the funds to operate their illegal money transmitting business in violation of Section 1960, which is also an SUA.

Finally, the court held that all property involved in the transactions, including any commingled funds from other sources, was subject to forfeiture as "property involved" in the money laundering offenses.

So, the Government's motion for a default judgment was granted. *SDC*

Contact: AUSA Chris Brown

Comment: First, this case illustrates once again the essential role that civil forfeiture plays when it is not possible to bring a successful criminal prosecution against an actor who remains outside of the United States.

Second, it is an example of the application of familiar money laundering concepts to the world of virtual currency. To the list of ways in which criminals can engage in concealment money laundering, the court adds the use of "peel chain" transactions whereby the perpetrator starts off which a large sum of cryptocurrency in one account, and successively peels off fractions of that sum in a long chain of transactions that end when there are no longer any funds to transfer. (For an explanation of "peel chain" transactions, *see* the opinion in *United States v. Sterlingov,* summarized below.)

In addition, to the list of ways in which a person can engage in promotional money laundering, the court adds the use of stolen virtual assets to run an unlicensed money transmitting business in violation of § 1960, and to pay for "site hosting from service provides that focus on client anonymity, and virtual private networks."

Finally, the court applies the well-established rule that the property subject to forfeiture in a money laundering case is not limited to the SUA proceeds being laundered but includes any commingled funds from other sources that are involved in the money laundering offense to the laundering of cryptocurrency. *SDC*

Investigative Tools / Searches and Seizures

Kim

Observation of a known money launderer leaving his residence with a large quantity of currency is sufficient probable cause to believe the residence will contain evidence of money laundering.

Court upholds the search of a money launderer's cell phone for photos, messages, and metadata based on evidence from confidential sources that he uses the phone to arrange money deliveries; no time limit on the age of the photos and messages to be seized need be specified.

The Fourth Amendment does not apply to the exterritorial search of a cryptocurrency trading account.

United States v. Kim, 2023 WL 8650268 (N.D. Ill. Dec. 14, 2023).

N.D. Ill. * Defendant, indicted for laundering drug money, moved to suppress the fruits of the search of his residence and his cell phone, and of the information obtained from a foreign cryptocurrency trader.

First, he argued that his connection with drug traffickers did not, by itself, provide probable cause to search his residence. The court agreed that that would be so as a general matter, but held that Defendant's having twice delivered large quantities of cash to undercover agents, and the observation of Defendant leaving his residence with a quantity of cash on a third occasion, provided the necessary probable cause to believe that the residence would contain evidence of money laundering.

Second, Defendant objected to the search of his cell phone for broad categories of information including photos and messages relating to money laundering, records of incoming and outgoing calls, and related metadata regarding the dates, times, and locations associated with the photos and messages. But the court held that evidence from witnesses developed in the course of the months-long investigation indicated that Defendant was using his cell phone to communicate about money deliveries including, on at least one occasion, that Defendant received a photo of the serial number on a dollar bill to use as a password.

To the extent that Defendant complained that the warrant put no time limit on the age of the photos and messages that were subject to seizure, the court held that where it is impossible for agents to know how far back a subject's criminal conduct goes, the warrant is sufficiently particular if it specifies the conduct under investigation without specifying a range of dates.

Finally, Defendant objected that an IRS agent obtained information from a cryptocurrency trading account with a business located in Finland without obtaining a warrant. But the court held that because the agent's conduct occurred outside of the United States, the Fourth Amendment did not apply.

So, Defendant's motion to suppress was denied. *SDC*

Contact: AUSA Richard Rothblatt

Pouryan

Defendant cannot use a Rule 41(g) motion to seek the return of property that was included in a criminal forfeiture order on grounds that he could have raised at the time the order was entered.

Defendant who did not object to the forfeiture of his cell phone cannot later object that the bitcoins stored on his cell phone had to be forfeited separately, and should be returned to him because they were not.

The statute of limitations for filing a Rule 41(g) motion is six years.

United States v. Pouryan, 2023 WL 8622160 (S.D.N.Y. Dec. 12, 2023).

S.D.N.Y. * Defendant, an arms trafficker with ties to Hezbollah, was convicted of providing material support to terrorists and ordered to forfeit a list of assets pursuant to 18 U.S.C. § 981(a)(1)(G). One of the listed assets was a cell phone that was seized from Defendant at the time of his arrest.

Defendant opposed the forfeiture order on Eighth Amendment grounds, but did raise any objection specifically related to the cell phone. The court overruled the Eighth Amendment objection and Defendant did not appeal.

Nine years later, Defendant filed a Rule 41(g) motion for the return of the cell phone, arguing for the first time that it contained 5,950 bitcoins, now worth $2 million. Because the bitcoins were not listed in the forfeiture order, he argued, they should be returned to him.

The court denied the motion for three reasons. First, because the statute of limitations for filing a Rule 41(g) motion for the return of seized property is six years, Defendant's motion was time barred.

Second, Defendant could not use Rule 41(g) to contest a forfeiture order on grounds that he could have raised at the time the order was imposed. While the bitcoins – if they existed (a point that the Government disputed) – were not listed on the Government's proposed forfeiture order, the cell phone itself was listed. So, if there were bitcoins on the cell phone and Defendant wanted to oppose their forfeiture, he needed to raise that objection before the forfeiture order was entered, which he did not.

Finally, the court held that because the cell phone has been destroyed, and because there is no evidence that it ever contained any bitcoins or that any were removed from it, there is nothing to return. Thus, Defendant's motion was moot. *SDC*

Contact: AUSA Jerry Jia-Wei Fang

Sterlingov

Court declines to order the Government to provide defendant accused of running a bitcoin tumbling business with a description of the methods the Government uses to detect bitcoin tumbling.

United States v. Sterlingov, ___ F. Supp.3d ___, 2023 WL 8365390 (D.D.C. Nov. 30, 2023).

D.D.C. * Defendant operated Bitcoin Fog, a bitcoin tumbling business that commingled bitcoin from different customers in a pooled account and then redistributed them to the customers, minus a fee. In so doing, Defendant's business made it difficult for law enforcement to trace a given quantity of bitcoin to its original source.

Defendant was indicted for conspiracy to commit money laundering and for operating an unlicensed money transmitting business, in violation of 18 U.S.C. §§ 1956(h) and 1960, respectively. To prepare his defense, he asked the Government to provide him with the details of the methods that the Government's expert, Chainalysis, uses to detect the presence of "coinjoin services" – which are attempts to combine cryptocurrency transactions in a way that disguises the fact that multiple transactions are attributable to the same person.

The court agreed with the Government that giving Defendant access to such information raised a "valid and substantial" concern. "Each disclosure of how the Government (or its experts) cluster or track bitcoin transactions," the court said, "ups the ante in the detection-evasion cat-and-mouse game." Indeed because Defendant himself is accused of designing a system that would allow users to "avoid clustering and tracing of their on-chain activities," the disclosure of the government's detection methods would undermine their utility to law enforcement.

Accordingly, the court issued a protective order providing that the Government's methods would be disclosed only to Defendant's counsel (and such experts as they needed to employ), but would not be disclosed to Defendant. *SDC*

Contact: AUSA Chris Brown

Sterlingov

Court conducts a Daubert *hearing and finds that the results of a blockchain analysis linking a defendant and his business to a cryptocurrency tumbling operation were sufficiently reliable to be admitted into evidence.*

United States v. Sterlingov, ___ F. Supp.3d ___, 2024 WL 860983 (D.D.C. Feb. 29, 2024).

D.D.C. * Defendant operated Bitcoin Fog, a bitcoin tumbling business that commingled bitcoin from different customers in pooled accounts and then redistributed them to the customers, minus a fee. In so doing, Defendant's business made it difficult for law enforcement to trace a given quantity of bitcoin to its original source.

When Defendant was indicted for conspiracy to commit money laundering and for operating an unlicensed money transmitting business, the Government provided expert discovery regarding the details of the methods that the Government's expert, Chainalysis, used to identify the 900,000 cryptocurrency addresses used by Bitcoin Fog to conduct its tumbling operation, and to link Bitcoin Fog to various darknet market sites.

At the Court's urging, the Government also provided a "highly confidential, supplemental production" containing more precise details of the Chainalysis clustering program. The court held that Defendant's counsel were entitled to such information, but issued a protective order that precluded them from revealing the details to Defendant or to the public. *United States v. Sterlingov*, ___ F. Supp.3d ___, 2023 WL 8365390 (D.D.C. Nov. 30, 2023) (February 2024 *Digest*).

Defendant then moved to exclude the evidence obtained from Chainalysis on the ground that its software program, known as Reactor, is "junk science" and does not yield reliable results. Accordingly, the court conducted a multi-day *Daubert* hearing to determine whether Reactor's results were reliable.

In a detailed and well-drafted opinion, the court explained the various ways in which Reactor is able to link a given person or business to an otherwise anonymous cryptocurrency address. Among other things, the program looks at transactions where the same person is drawing cryptocurrency from multiple addresses at the same time, which gives rise to the assumption that the same person has the "private key" to all of those addresses. Thus, if the owner of one address is known, the owner of the other addresses is known as well.

Also, the court explained how Reactor looks for telltale signs that similar transactions are being conducted in the same way, thus indicating that the person conducting one transaction is likely the person conducting the other transactions as well.

Finally, the court discussed how Reactor's results are verified or corroborated by comparing the results with the information obtained via subpoena, searches of a suspect's computer, undercover transactions, or information obtained from informants or other sources. According to the experts who testified at the Daubert hearing, there was never a time when the link provided by Reactor to a given individual yielded a false positive or was otherwise found to be incorrect.

Based on this evidence, the court found that the data provided by Reactor that linked Defendant and Bitcoin Fog to the multitude of cryptocurrency addresses was "not junk science," but was sufficiently reliable to be admitted into evidence and presented to the jury. Defendant remained free, the court noted, to attack the evidence at trial through cross-examination of witnesses and by presenting contrary evidence; but under the *Daubert* standard, the court said, it "clears the standard necessary to reach the jury."

So, Defendant's motion to exclude the analysis obtained from Chainalysis was denied. SDC

Contact: AUSA Chris Brown

Comment: For anyone struggling to understand how Chainalysis and its cohorts in the blockchain analysis business are able to link – with a high degree of reliability – a given person to a constellation of seemingly anonymous cryptocurrency addresses, this opinion is the place to start. It is a stellar example of expository writing, making it possible for a layperson to understand both how the analysis is done and why it is reliable – and accordingly, why the results are admissible as evidence in a criminal trial under the *Daubert* standard. *SDC*

Payward Ventures

Court agrees to enforce IRS summons to Kraken, a digital currency exchange, requiring it to produce customer identification data and transaction records for customers with over $20,000 in their accounts.

United States v. Payward Ventures, Inc, 2023 WL 4303653 (N.D. Cal. Jun. 30, 2023).

N.D. Cal. * In 2021, the IRS sent a summons to Payward Ventures, d/b/a Kraken, a digital currency exchange, seeking information regarding customers who had any combination of accounts having at least $20,000 in value in any one year between 2016 and 2020. When Kraken objected to the summons on relevance and burdensomeness grounds, the IRS commenced an enforcement action pursuant to 26 U.S.C. §§ 7402(b) and 7604(a).

In a lengthy opinion reciting in detail the arguments made by both sides, the court held that the summons was enforceable in part.

First, the court held that the IRS had a valid basis for requesting the customer information. "The number of taxpayers filing tax returns with a property description related to bitcoin between 2016 and 2020," the court said, while numbering in the tens of thousands, "is still dwarfed by the amount of trading activity that occurs on Kraken," which has over four million clients. Accordingly, the information requested by the IRS was likely to be relevant to its mission of ensuring tax compliance by persons engaging in cryptocurrency transactions.

The court then held that the IRS was entitled to request basic information, including the name, date of birth, taxpayer identification number, physical address, phone number, and email address of its customers. It also held that with respect to transactions conducted by customers who fell within the scope of the summons, the IRS could request transaction ledgers and data showing the date, time, dollar value, transaction hash (ID), and blockchain address for each transaction.

It held, however, that the summons was overbroad to the extent that it requested customer histories, payment methods (e.g. bank account information), KYC questionnaires, and exception reports produced by Kraken's AML system. Such records, the court said, could be requested in a follow-up summons if they appeared to be relevant for a given customer once the IRS reviewed the response to the initial subpoena. *SDC*

Contact: Tax Division Attorney Amy Matchison

Comment: Several years ago, the IRS issued a similar summons to Coinbase, another digital currency exchange, that resulted in a similar order enforcing the summons in part, but requiring the IRS to issue a second-round of summonses for follow-up information if it turned out to be needed. *United States v. Coinbase, Inc.,* 2017 WL 5890052 (N.D. Cal. Nov. 28, 2017). Much of the argument in this case dealt with whether the ruling in *Coinbase* was too narrow, or whether based on the IRS's experience in that case, it was appropriate to enforce a summons that sought a wider range of information. In particular, the IRS argued that having to issue multiple rounds of summons – rather than being able to request all of the relevant information at one time – had hampered and delayed its investigation.

In the end, however, the magistrate judge mostly followed the holding in *Coinbase,* but did grant the IRS somewhat more latitude in a few respects. *SDC*