A Shot in the Dark: Using Asset Forfeiture Tools to Identify and Restrain Criminals' Cryptocurrency

Shirley U. Emehelu
Chief, Asset Recovery and Money Laundering Unit
United States Attorney's Office
District of New Jersey

I. Introduction

Over the past decade, law enforcement has witnessed a rise in the use of various forms of cryptocurrency in wide ranging types of criminal enterprises—including drug trafficking, child exploitation, human trafficking, financial fraud, and money laundering schemes, to name just a few. Cryptocurrency offers many benefits to those engaged in criminal activities including anonymized payment transactions; the elimination of the need to transport bulky quantities of cash to fund and launder the proceeds of criminal activity; a transnational form of currency that can be used globally; the ability to engage in speculation arising from potential spikes in the value of cryptocurrency; and relatively low financial regulation compared to heavily regulated forms of traditional currency. This article demonstrates the impactful role that asset forfeiture can play in effectively investigating and prosecuting crimes involving cryptocurrency.

A. The advantages of asset forfeiture

Asset forfeiture is an integral part of federal criminal law enforcement. It can serve as a powerful tool in cases involving cryptocurrency as the spoils of the crime or the currency driving the crime.

In this area (as in many others), a number of critical objectives are achieved through asset forfeiture. Asset forfeiture removes the instrumentalities of crime from the control of wrongdoers. Such instrumentalities may include cryptocurrency, which, although not illegal in and of itself, can provide criminals the ability to fund criminal schemes and launder the proceeds thereof with relative anonymity. In addition, asset forfeiture is a crucial mechanism for

recovering assets that may be used to compensate innocent victims in cases involving property offenses and fraud. In such cases, asset forfeiture allows for the preservation of assets, such as cryptocurrency, during the pendency of the criminal case so that the assets can be liquidated and the funds restored to victims for restitution.[1]

Asset forfeiture also takes the profit out of crime by removing the fruits of illegal crimes—such as cryptocurrency—from the hands of wrongdoers. This sends a deterrent message to those contemplating engaging in economic crime by increasing the risk that a criminal will be stripped of his ill-gotten gains. Finally, asset forfeiture serves as a form of punishment by depriving a convicted wrongdoer of the assets that provided the wrongdoer the means with which to commit the criminal activity and the spoils that came with accomplishing the criminal scheme.

In order to be able to realize these important objectives, there first must be statutory grounds to pursue asset forfeiture in a given case. For example, there may be statutory authority to seize cryptocurrency as the proceeds of the criminal offense;[2] the payment source used or intended to be used to purchase a controlled substance;[3] property involved in a money laundering offense;[4] property acquired or maintained through racketeering activity;[5] or the property of an individual engaged in planning or committing acts of domestic or

---

[1] *See* 18 U.S.C. § 981(e)(6) (authorizing the government, in civil forfeiture cases, to use forfeited property to pay restitution to the victims of the underlying crimes); 21 U.S.C. § 853(i) (authorizing the same for criminal forfeiture).

[2] *See, e.g.*, § 981(a)(1)(C) (authorizing the forfeiture of the proceeds of a long list of state and federal crimes, including fraud, bribery, embezzlement, and theft); § 853(a)(1) (outlining property subject to criminal forfeiture); 21 U.S.C. § 881(a)(6) (authorizing the forfeiture of the proceeds of drug offenses).

[3] *See* § 881(a)(6) (subjecting to forfeiture, inter alia, all moneys, negotiable instruments, securities, or other things of value furnished or intended to be furnished by any person in exchange for a controlled substance, and all proceeds traceable to such an exchange).

[4] *See* § 981(a)(1)(A) (civil forfeiture); 18 U.S.C. § 982(a)(1) (criminal forfeiture).

[5] *See* 18 U.S.C. § 1963(a).

international terrorism, regardless of whether the cryptocurrency was involved in the terrorism activity.[6]

As set forth below, identifying and seizing forfeitable cryptocurrency requires careful planning by prosecutors and their law enforcement partners.

B. Cryptocurrency terms

Before discussing law enforcement techniques for identifying and seizing cryptocurrency, it is important first to understand certain key concepts related to cryptocurrency.

1. Centralized vs. decentralized digital currency

Cryptocurrency, also known as "digital currency" or "virtual currency," is generally defined as "a digital unit of exchange that is not backed by a government-issued legal tender."[7] The first digital currencies were "centralized," meaning that they were controlled by centralized, private entities.[8] A few examples of these early, centralized digital currencies were E-gold, a digital currency purportedly backed by gold bullion, and Liberty Reserve, an online payment system in which users transacted in digital currency.[9] Both E-gold and Liberty Reserve ultimately were prosecuted and/or shut down by law enforcement for facilitating wide scale money laundering.[10]

---

[6] *See* § 981(a)(1)(G) (conferring extremely broad forfeiture authority that allows the government to seize and forfeit *all* assets, foreign or domestic, of a terrorism defendant).

[7] *Virtual Economies and Currencies: Additional IRS Guidance Could Reduce Tax Compliance Risks* at 3 (U.S. GOVERNMENT ACCOUNTABILITY OFFICE May 2013) [hereinafter GAO REPORT].

[8] Lawrence Trautman, *Virtual Currencies Bitcoin & What Now After Liberty Reserve, Silk Road, and Mt. Gox?*, 20 RICH. J.L. & TECH. 13, at *5 (2014).

[9] *Id*.

[10] In July 2008, E-Gold Ltd. (E-Gold), its corporate affiliate Gold & Silver Reserve Inc., and its three principal directors and owners—Douglas Jackson, Barry Downey, and Reid Jackson—pled guilty to criminal charges relating to money laundering and the operation of an illegal money transmitting business. *See* Press Release, U.S. Dep't of Justice, Digital Currency Business E-Gold Pleads Guilty to Money Laundering and Illegal Money Transmitting Charges (July 21, 2008). As for Liberty Reserve, law enforcement shut down the digital currency payment system in May 2013, as it had grown into a financial hub for criminal actors around the world, who used it "to amass,

In contrast, "decentralized" digital currencies "have no centralized administrating authority and instead operate as peer-to-peer transaction networks[.]"[11] Bitcoin, the first decentralized cryptocurrency emerged around 2009. Bitcoin remains the world's most widely used virtual currency. Several other cryptocurrencies have emerged, such as Monero, Ethereum, Dash, and Litecoin.[12]

Figure 1: Cryptocurrencies and Respective Icons

2. Blockchain transactions

Using a peer-to-peer network, an owner of Bitcoin or other similar cryptocurrency may make an online payment to another party without going through a financial institution. Unlike traditional or "fiat" currencies, cryptocurrencies are not minted or printed by a central government or agency. Instead, cryptocurrencies like Bitcoin are "mined" by "miners," members of the cryptocurrency network who offer their computers' processing power to solve mathematical

---

distribute, store, and launder criminal proceeds of their [online Ponzi schemes], including proceeds of investment fraud, credit card fraud, identity theft, and computer hacking." Press Release, U.S. Dep't of Justice, Founder of Liberty Reserve Pleads Guilty to Laundering More Than $250 Million (Jan. 29, 2016). By the time it was shut down, Liberty Reserve had five million user accounts worldwide, including more than 600,000 accounts associated with users in the United States, and had processed millions of transactions. *Id.* In January 2016, Arthur Budovsky, the founder and operator of Liberty Reserve, pled guilty in federal court to conspiring to commit money laundering, admitting that he had laundered between $250 million and $550 million in criminal proceeds linked to Liberty Reserve accounts based in the United States. *Id.* Budovksy was sentenced, in May 2016, to 20 years in prison for his massive money laundering enterprise. *See* Press Release, U.S. Dep't of Justice, Liberty Reserve Founder Arthur Budovsky Sentenced in Manhattan Federal Court (May 6, 2016).

[11] Trautman, *supra* note 8, at *5 (citation omitted).

[12] Alex Hern, *Everything You Wanted to Know About Bitcoin But Were Afraid to Ask*, THE GUARDIAN, Nov. 11, 2017.

equations confirming that the sender of funds in each transaction has the right to spend the specific cryptocurrency involved. This mining process yields a general ledger of transactions that are publicly accessible on the Internet. This publicly available ledger is called "blockchain"—a list, or "block," of transactions that are made during a set period of time that includes the unique hash for each block. [13] "A 'hash' is a unique random sequence of letters and numbers that is shorthand for a unique transaction between users that is stored with the block."[14] The blockchain prevents an individual from using already spent cryptocurrency to transact with someone else. Each new block incorporates the prior block's hash.[15]

3. Public vs. private key

There are two important components of cryptocurrency transactions: the "public key" and the "private key." A public key or public address, which may be thought of as a bank account number, is shared by a Bitcoin[16] user with other individuals from whom the user would like to receive Bitcoin payment. The private key, which is akin to an ATM pin number, enables the user to send or spend Bitcoin from his or her Bitcoin wallet.[17]

The publically accessible blockchain, which evidences the validation and settling of cryptocurrency transactions, does not identify the users' actual names, personal identifying information, or their private keys. The blockchain does, however, include the Bitcoin address, or public key, of the sending and receiving parties, the amount of the transaction, IP addresses, the date and time of the transaction, and other information.[18]

4. Cryptocurrency wallets

Wallets are software programs that interface with blockchains and generate and/or store public and private keys used to send and receive

---

[13] Christopher Burks, *Bitcoin: Breaking Bad or Breaking Barriers?,* 18 N.C. J. L. & TECH. 244, 248–49 (2017).
[14] *Id*. at 249 n.18.
[15] *Id.* at 249.
[16] Although there are now many forms of cryptocurrency, Bitcoin will predominantly be referred to here, given that it is the most commonly used type of cryptocurrency.
[17] *A Beginner's Guide to Blockchain Technology*, COINDESK, https://www.coindesk.com/information/.
[18] *Id*.

cryptocurrency. There are a plethora of different types of wallets, which offer varying levels of, among other things, value, convenience, risk of loss, and anonymity. Whoever possesses the private key has unrestricted access to the cryptocurrency in the wallet. Without the private key, access to the cryptocurrency cannot be obtained.[19]

Some wallets are browser-based, meaning that they are hosted and serviced by providers via the Internet. Alternatively, a software client downloaded on a user's computer can be used to access a wallet, or users may access wallets via a mobile device or smartphone by downloading an application from a wallet provider.[20]

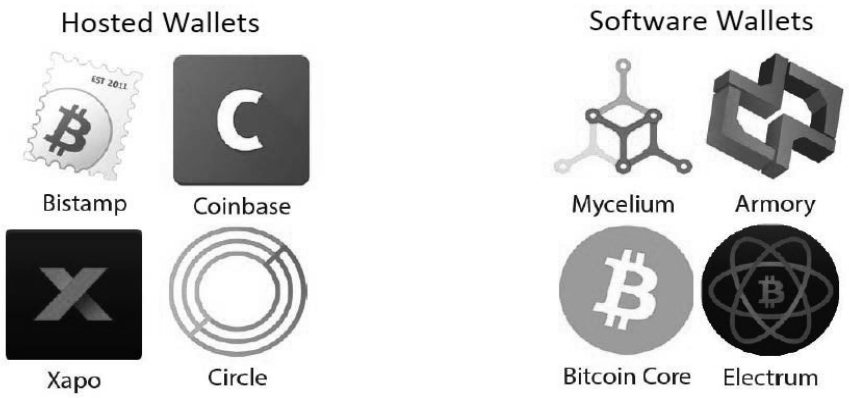

Figure 2: Examples of Cryptocurrency Wallets

[19] *Id.*
[20] *Id.*

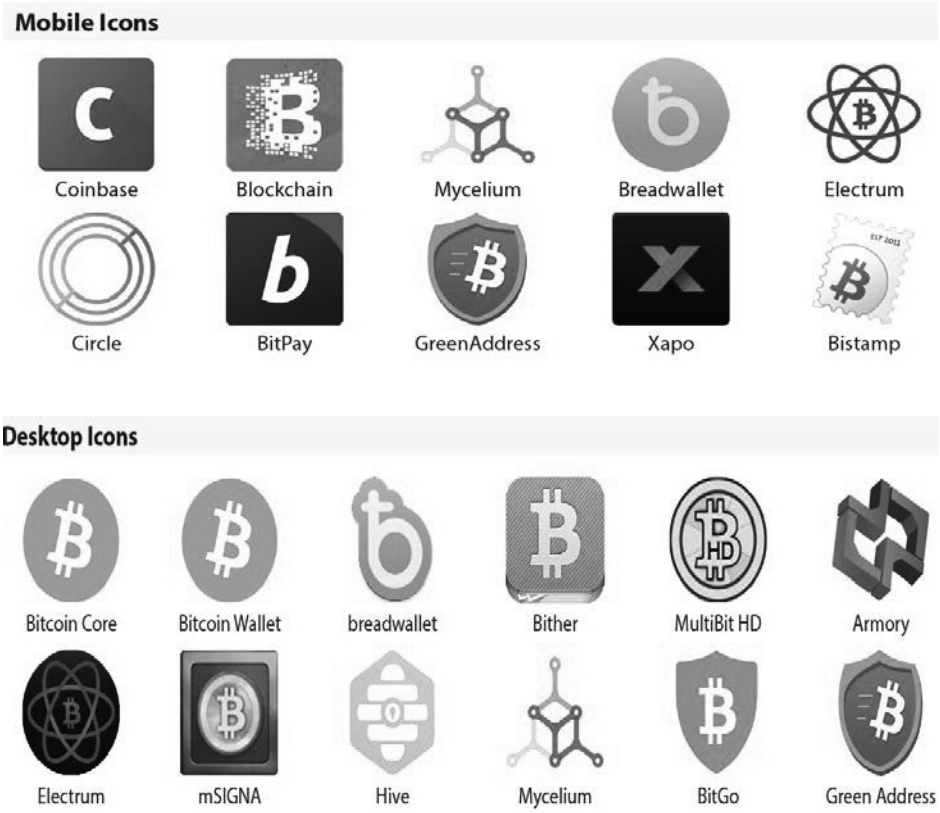

Figure 3: Icons Depicting Various Wallet Programs

A user may also effect cryptocurrency transactions by sharing a public key or address with other users via a Quick Response (QR) Code, which is a barcode that can be scanned by technologies available on many smartphones and other devices.[21]

Wallets themselves come in different forms—for example, a paper wallet is simply the user's private and public key memorialized on paper. Alternatively, a user can obtain a physical coin that is preloaded with the value of the cryptocurrency. With a brain wallet, the user's private key is encrypted into a phrase for the user to recall through the use of third party software that generates a phrase associated with a private key. Finally, a "cold storage" wallet stores the cryptocurrency offline, for example on a hardware device.[22]

[21] *Id.*
[22] *Id.*

Figure 4: Forms of Wallets for Cryptocurrency

5. Cryptocurrency exchanges

A cryptocurrency exchange provides customers the ability to buy and sell cryptocurrency using traditional currency—transacting either with the exchange or among themselves—and the exchange also may allow a customer to exchange one type of cryptocurrency for another (for example, exchanging Bitcoin for Monero).[23]

6. The dark web

The "dark web" is a portion of the "Deep Web" of the Internet, where individuals must use an anonymizing software of application called a "darknet" to access content and websites. The Deep Web is the portion of the Internet not indexed by search engines. Examples are databases and internal networks belonging to private industry, government agencies, or academic institutions. Within the dark web, criminal marketplaces operate, allowing individuals to buy and sell illegal items—often with cryptocurrency as the preferred method of payment—such as drugs, firearms, and other hazardous materials, with greater anonymity than is possible on the traditional Internet (sometimes called the "clear web" or simply the "web"). These online market websites use a variety of technologies, including the Tor network (defined below) and other encryption technologies, to ensure that communications and transactions are shielded from interception and monitoring.[24] Famous dark web marketplaces such as Silk Road, AlphaBay, and Hansa (all of which have since been shut down by law

[23] *Id.*

[24] *See generally* DANIEL SUI, ET AL., WILSON CENTER, SCI. & TECH. INNOVATION PROGRAM, THE DEEP WEB AND THE DARKNET: A LOOK INSIDE THE INTERNET'S MASSIVE BLACK BOX (Aug. 2015).

enforcement), operated similarly to clear web commercial websites such as Amazon and eBay, but offered illicit goods and services.

The "Tor network" or simply "Tor" (an abbreviation of "The Onion Router"), is a special network of computers on the Internet, distributed around the world, designed to conceal the true Internet Protocol (IP) addresses of the computers accessing the network, and, thereby, the locations and identities of the network's users. Tor also enables websites to operate on the network in a way that conceals the true IP addresses of the computer servers hosting the websites, which are referred to as "hidden services" on the Tor network.[25]

II. Forfeiting cryptocurrency

With key terms defined, we can now discuss the investigative mechanics of identifying and seizing forfeitable cryptocurrency. A comprehensive seizure plan is critical to ensuring the seamless identification, seizure, preservation, and liquidation of forfeitable cryptocurrency.

A. Identifying cryptocurrency transactions

The determination of whether a subject is transacting in cryptocurrency in connection with a criminal scheme is often made during the investigative stage, through the review of financial records of the subject. This financial records review may reveal transactions with cryptocurrency service providers such as cryptocurrency exchangers, payment processors, and wallet providers. Once particular cryptocurrency service providers are identified from financial records, those third-party service providers can be subpoenaed for customer account records, which may help identify suspicious cryptocurrency transactions involving the subject.

The open-source nature of blockchain transactions also facilitates an investigator's determination of whether a criminal subject has transacted in cryptocurrency. There are various online tools, called blockchain or block "explorers," that are publicly available on the Internet that enable one to search the data contained in the blockchain. Thus, for example, if an investigator learns of a Bitcoin address associated with a particular scheme, the investigator can search the address through a blockchain explorer in order to locate possible Bitcoin transactions involving that particular address. The block explorer search can reveal the following transactional

[25] *Id.*

information: the Bitcoin transaction ID and Date/Time Stamp (in Universal Coordinated Time/UTC), the amount of Bitcoin (BTC) transacted, the sender's public key or Bitcoin address, and the receiver's public key or Bitcoin address. IP address information may also be revealed, but the IP addresses may not be the true locations of the Bitcoin senders and receivers, because many exchangers and wallet providers may use proxy IPs or IPs that do not constitute the true location of the computer or device used to access the Bitcoin network to carry out the transaction. That being said, if an investigator is aware of a particular IP address utilized by a subject, the investigator can use that IP address to execute a search using the block explorer online tool to identify any cryptocurrency transactions executed using that IP address.

Once a suspicious cryptocurrency transaction has been identified, and if it is determined that the transaction was effected through a cryptocurrency payment processor, a subpoena can be issued to the payment processor requesting, among other things, any wallet address(es) associated with the transaction, any bank account number(s) registered to the user, and any personal information linked to the account user (for example, name, email, address, phone number, IP logs, and credit card information).

Court-issued search warrants for email and text message content stored by third party electronic service providers also can yield information related to a subject's engagement in cryptocurrency transactions. Such records may reveal communications with cryptocurrency exchanges, wallet-service providers, individuals desirous of engaging in cryptocurrency transactions, and other evidence of cryptocurrency usage.

Law enforcement review of communications and contraband trafficking on Darknet markets or websites can also produce valuable information regarding a subject's cryptocurrency usage, since cryptocurrency is generally the currency of choice for criminals on the Darknet.

B. Seizure of cryptocurrency

Thus far, we have discussed some covert methods for obtaining information regarding a criminal subject's engagement in cryptocurrency transactions. Next, we will discuss how to prepare for the overt stage of an investigation in light of a criminal subject's cryptocurrency usage, so that said cryptocurrency can be effectively seized and preserved during the pendency of the criminal case.

The central objective for seizing cryptocurrency that was stolen or used to facilitate criminal activities is gaining access to a subject's private key. The private key may be controlled by (1) a wallet installed on the subject's computer, smartphone, or an external storage device such as a hardware wallet or a USB drive; (2) a paper wallet or memorialized on a piece of paper; and/or (3) a third party such as a cryptocurrency exchanger or online wallet provider. Therefore, court-issued search warrants for the subject's residence, business, cellular telephone, and person should include wallets and evidence of the private key among the items to be seized. Forfeiture seizure warrants, court-issued pursuant to 18 U.S.C. §§ 981(b) and 982(b), 21 U.S.C. § 853(f), and 21 U.S.C. § 881(b), may be served on third-party custodians of a subject's cryptocurrency such as exchangers and online wallets if the cryptocurrency is statutorily subject to forfeiture based on the criminal offense or offenses that the subject is suspected of committing.

The investigator's job is not complete with the recovery of the subject's private key data, since the subject or an associate with access to the private key can simply move the cryptocurrency to another address. The investigator must be readily prepared to transfer the cryptocurrency into a secure wallet controlled by law enforcement. Thus, effective seizure planning will require that law enforcement wallet(s) be in place prior to seizure, and the address(es) for the wallet(s) should be readily accessible to law enforcement so that the subject's cryptocurrency can be transferred without delay on the day of the takedown. This is particularly important where the subject's cryptocurrency wallets are encrypted, which may require exporting the private keys from the subject's computer or device while it is online and running.

Law enforcement interviews of subjects should include in-depth questioning regarding the subject's cryptocurrency usage, including but not limited to the types of wallets, payment processors, and/or exchangers used by the subject, the location of wallets, private key information, and passwords for encrypted wallets.

Prosecutors moving to compel a defendant to disclose his or her encryption password or private key face litigation risk, since there is a dearth of case law dealing with compelled decryption. There do not appear to be any reported cases dealing with compelled disclosure of cryptocurrency private keys, and the holdings of the cases that do address compelled decryption are contradictory. In what appears to be the earliest reported case addressing the constitutionality of

compelled decryption, the government sought to decrypt the Z-drive of the defendant's laptop, the contents of which the defendant had allowed an agent to search before the defendant's arrest for knowing transportation of child pornography and the seizure of the laptop, which was shut down after seizure.[26] A search warrant was obtained for the laptop, but during the course of creating a mirror image of its contents, the government discovered that it could not find or open the Z-drive. A grand jury subpoena was issued directing the defendant to produce the password, and the defendant moved to quash the subpoena. During oral argument and in post-argument submissions, the government stated that it intended only to require the defendant to provide an unencrypted version of the drive to the grand jury, in lieu of the password itself.

In adjudicating the defendant's motion to quash, the court considered the United States Supreme Court's holdings in several other cases to determine the central question: "whether requiring Boucher to produce an unencrypted version of his laptop's Z drive would constitute compelled testimonial communication."[27] Applying the "foregone conclusion" doctrine,[28] the court in *Boucher* concluded that compelling decryption did not constitute compelled testimonial communication because the government previously knew the location of the Z-drive and its files since the defendant allowed the agent to view the contents of the Z-drive, upon which the agent determined that it appeared to contain images or videos of child pornography.[29] Thus, the court reasoned, the defendant's act of producing an unencrypted version of the Z drive was not necessary to authenticate it because he already admitted to possessing the computer and provided the government with access to the Z drive.[30] Since *Boucher* was decided, courts have reached mixed holdings.[31]

---

[26] *In re* Boucher, No. 2:06-mj-91, 2009 WL 424718, at *1 (D. Vt. Feb. 19, 2009).

[27] *Id.* at *3 (considering Fisher v. United States, 425 U.S. 391 (1976), United States v. Doe, 465 U.S. 605 (1984), Doe v. United States, 487 U.S. 201 (1988), and United States v. Hubbell, 530 U.S. 27 (2000)).

[28] *See Fisher*, 425 U.S. at 411.

[29] *In re Boucher*, 2009 WL 424718, at *4.

[30] *See id.*

[31] *See, e.g.,* United States v. Kirschner, 823 F. Supp. 2d 665 (E.D. Mich. 2010) (quashing a subpoena ordering the defendant to provide all passwords associated with computer and any files on it based on court's finding that providing the government access to his encrypted files would violate his

C. Establishing the forfeitability of seized cryptocurrency

Seized cryptocurrency is maintained in the custody of the U.S. Marshals Service in secure wallet(s) pending the resolution of the criminal case and the adjudication of the cryptocurrency's forfeitability, which is determined in accordance with the same procedural rules that govern the adjudication of the forfeitability of any form of specific property in a criminal case.

Criminal forfeiture procedure is discussed herein, but the government may seek civil forfeiture in parallel with, or in lieu of, criminal forfeiture. In a civil forfeiture case, the government files a civil action in rem against the property itself, and must prove by a preponderance of the evidence that the property was derived from or was used to commit a crime. Thus, unlike criminal forfeiture, civil forfeiture does not depend on a criminal conviction and civil forfeiture may proceed even if the defendant property belongs to a fugitive, someone who has died, or where the government can prove that the property was involved in a crime but cannot identify the wrongdoer.[32]

---

privilege against self-incrimination); United States v. Fricosu, 841 F. Supp. 2d 1232 (D. Colo. 2012) (holding the Fifth Amendment privilege was not applicable where defendant declined to produce the unencrypted contents of her laptop, since the contents of the laptop and facts communicated by the production of those contents were foregone conclusions, where the government knew of the existence and location of the computer's files, notwithstanding the government's lack of knowledge as to the specific contents of said files); *In re* Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011, 670 F.3d 1335 (11th Cir. 2012) (reversing district court's contempt holding for defendant's refusal on Fifth Amendment grounds to comply with a subpoena requiring defendant to appear before a grand jury and produce the unencrypted contents of his hard drives, and rejecting the foregone conclusion argument given that the government's mere possession of the hard drives did not mean it knew of the existence and location of the electronic files stored therein, and because the decryption and production of the contents of the hard drives would form a link in the chain of evidence that would lead to incriminating evidence).

[32] *See, e.g.*, United States v. One-Sixth Share Of James J. Bulger In All Present And Future Proceeds Of Mass Millions Lottery Ticket No. M246233, 326 F.3d 36, 40 (1st Cir. 2003) ("Because civil forfeiture is an in rem proceeding, the property subject to forfeiture is the defendant. Thus, defenses against the forfeiture can be brought only by third parties, who must intervene.").

Procedurally, civil forfeiture actions are closely akin to other civil cases. They commence with a verified complaint filed by the government as plaintiff; claimants are then required to file claims to the property and answer the complaint within a certain period of time; followed by civil discovery, motions practice, and trial—by jury if the right is asserted by a claimant with standing—with the government bearing the burden of establishing the forfeitability of the property by a preponderance of the evidence.[33]

1. Forfeiture allegations in charging document

At the start of the criminal case, the indictment or information must include forfeiture allegations providing notice to the defendant that the government will seek the forfeiture of property as part of any sentence in accordance with the applicable forfeiture statute.[34] The forfeiture allegation should list any property believed to be subject to forfeiture that "includes but is not limited to,"[35] specifically itemized property such as cryptocurrency.

2. Guilty plea convictions

Forfeiture is not judicially adjudicated until after the defendant has been convicted of an offense or offenses supporting forfeiture. If the conviction is by guilty plea, the plea agreement should include forfeiture language setting forth the defendant's agreement to the entry of any forfeiture money judgment and the forfeiture of specific property such as cryptocurrency. The prosecutor should also submit a preliminary order of forfeiture to the court for entry at the plea hearing or shortly thereafter. The preliminary order of forfeiture mirrors the forfeiture stipulations in the plea agreement, setting forth the amount of any forfeiture money judgment and directing the forfeiture of specific property, which would include any forfeitable cryptocurrency.[36]

3. Bifurcated trial procedures

If the defendant elects to go to trial, the court conducts the "forfeiture phase" as part of a bifurcated trial, whereby the "guilt

---

[33] *See generally* 18 U.S.C. § 983; FED. R. CIV. P., SUPP. R. G.
[34] *See* FED. R. CRIM. P. 7(c)(2); FED. R. CRIM. P. 32.2(a).
[35] Using this language allows the prosecutor to later add newly discovered property via a bill of particulars, without superseding the indictment.
[36] *See* FED. R. CRIM. P. 32.2(b)(2).

phase" of the trial is first held and the jury determines whether the defendant is guilty of the underlying criminal charges. If the jury returns a guilty verdict, either side (the government or the defendant) must make a specific and timely request to have the forfeiture phase go before the jury; otherwise, the court will adjudicate the forfeiture phase of the trial.[37] The trier-of-fact (whether the court or the jury) then must determine whether the government has established by a preponderance of the evidence that there is a "nexus" between the specific property that the government seeks to forfeit (for example, cryptocurrency), and the offense(s) of conviction.[38] The trier-of-fact may consider evidence already in the record—whether, for example, from the guilt phase of a trial or in a written plea agreement of a co-defendant—or made after an evidentiary hearing.[39]

If the government seeks a personal money judgment for the amount of proceeds personally obtained by the defendant from the criminal conduct supporting forfeiture, or the value of funds involved in a charged money laundering offense, "the court must determine the amount of money that the defendant will be ordered to pay."[40] Once the forfeiture phase is concluded and the trier-of-fact determines that property and/or any amount of money is subject to forfeiture, the court must promptly enter a preliminary order of forfeiture setting forth the amount of any money judgment and/or directing the forfeiture of specific property, which could include cryptocurrency.[41]

4. Substitute assets

A major advantage of criminal (as opposed to civil) forfeiture is that the government may seek to forfeit "substitute assets" (legitimate assets of a defendant that are equivalent in value to the directly

---

[37] FED. R. CRIM. P. 32.2(b)(4).

[38] *See, e.g.*, United States v. Garcia-Guizar, 160 F.d 511, 518 (9th Cir. 1998); *see also* FED. R. CRIM. P. 32.2(b)(1).

[39] FED. R. CRIM. P. 32.2(b)(1).

[40] FED. R. CRIM. P. 32.2(b)(1)(A). Courts are split as to whether Rule 32.2(b)(4) provides a defendant the right to a jury trial regarding the amount of a money judgment. *Compare* United States v. Tedder, 403 F.3d 836, 841 (7th Cir. 2005) (finding no right to jury trial for determination of amount of money judgment), *with* United States v. Armstrong, No. CRIM 05-130, 2007 WL 809508, at *4 (E.D. La. Mar. 14, 2007) (overruling defense objection to government request for jury trial on amount of the money judgment).

[41] FED. R. CRIM. P. 32.2(b)(2).

forfeitable property) upon demonstrating that, by the defendant's own act or omission, the directly forfeitable property has been rendered unavailable for criminal forfeiture for any one of five specific reasons.[42] Such substitute assets could potentially include cryptocurrency that is not directly traceable to the criminal offense(s) of conviction. Once any untainted assets of a convicted defendant are located, the government may ask the court to amend the order of forfeiture to include forfeiture of that property.[43]

5. Third parties/ancillary proceedings

After the court issues a preliminary order of forfeiture, whether pursuant to a conviction by a guilty plea or after trial, the government must commence an ancillary proceeding to address any non-defendant, third party interests in the specific property forfeited, which could include third party interests of forfeited cryptocurrency.[44] The government is required to publish notice of the preliminary order and of its "intent to dispose of the property in such manner as the Attorney General . . . direct[s]" and "to the extent practicable, provide direct written notice to any person known to have alleged an interest in the [forfeited] property[.]"[45] The publication of notice should be executed in a manner consistent with the requirements of Supplemental Rule G(4)(a) of the Supplemental Rules for Admiralty or Maritime Claims and Asset Forfeiture Actions (hereinafter Supplemental Rule G). In addition, the government must send direct written notice to any known person who appears to have an interest in the forfeited property, and such notice may be sent by any of the applicable means described in Supplemental Rule G(4)(b)(iii). The notice provides non-defendant third parties the opportunity to file a petition with the court asserting their interests to the forfeited property.

If a third party files a petition asserting an interest in the forfeitable property—whether it be cryptocurrency or some other property—the court must conduct an ancillary proceeding.[46] Upon motion of the government, the court, assuming the facts set forth in the petition are true, may dismiss the petition for lack of standing, for failure to state

---

[42] *See* 21 U.S.C. § 853(p); 18 U.S.C. § 1963(m).
[43] FED. R. CRIM. P. 32.2(e)(1).
[44] § 853(n)(1); § 1963(l)(1).
[45] § 1963(l)(1); § 853(n)(1).
[46] FED. R. CRIM. P. 32.2(c)(1).

a claim, or for any other legal reason.[47] If the third party claims that he or she is the true owner of an interest in all or part of the property—for example, cryptocurrency—the third party bears the burden of proving either: (1) he or she holds a superior interest to that of the convicted defendant and that interest vested before the government's interest arose upon commission of the crime subjecting the property to forfeiture; or (2) he or she qualifies as a "bona fide purchaser for value" of the property, and had no knowledge, or grounds to know, that the property was subject to forfeiture when purchased or acquired.[48] Prior to holding a hearing on the petition, the court may allow the parties to conduct discovery in accordance with the Federal Rules of Civil Procedure, so long as the court concludes that discovery is necessary or desirable to resolve disputed factual issues.[49] Upon the conclusion of discovery, either party may move for summary judgment pursuant to Federal Rule of Civil Procedure 56. If multiple third party petitions are filed in the same case, an order dismissing or granting one petition cannot be appealed until the court rules on all the petitions, unless the court determines there is no justification for delay.[50]

6. Final order of forfeiture

When the ancillary proceeding has concluded, the court enters a final order of forfeiture by amending the preliminary order, if necessary, to resolve any third party rights to property.[51] In a simple, straightforward case, no third party interests are asserted and the government can submit a proposed final order of forfeiture at or before sentencing.

Generally, seized cryptocurrency is not liquidated until a final order of forfeiture is entered in the criminal case. In the simplest scenario, no third party interests are asserted and a final order of forfeiture is entered at or shortly before sentencing. Any third party claims to the seized cryptocurrency must be adjudicated through the ancillary claims process described above, and any resolved interests should be reflected in the final order of forfeiture. The final order of forfeiture must be made part of the sentence and be included in the Court's

---

[47] FED. R. CRIM. P. 32.2(c)(1)(A).
[48] *See* § 1963(l)(6); § 853(n)(6).
[49] FED. R. CRIM. P. 32.2(c)(1)(B).
[50] FED. R. CRIM. P. 32.2(c)(3).
[51] FED. R. CRIM. P. 32.2(c)(2).

judgment.[52] At sentencing, the preliminary order of forfeiture becomes final as to the defendant. If the defendant is required to forfeit specific property (such as cryptocurrency) under the order, and third party claims to said property have not been adjudicated in the ancillary proceeding as of sentencing, the forfeiture order will remain preliminary as to third parties until the ancillary proceeding is concluded.[53]

D. Liquidation of forfeited cryptocurrency

Once the forfeitability of seized cryptocurrency is finally adjudicated and a final order of forfeiture has been entered, the Marshals may commence the process of liquidating the seized cryptocurrency through its auction process. The forfeited cryptocurrency from a particular case will likely be pooled with forfeited cryptocurrency from other cases for auction. Auctions are held on a periodic basis, and thus there may be a lag time between the entry of a final order of forfeiture as to specific property that includes cryptocurrency, and the auction of said cryptocurrency.

The Marshals publish a public notice describing the particular type and quantity of cryptocurrency available for sale and inviting parties to submit a bid for purchase pursuant to specified instructions and eligibility requirements. The notice may reference the specific cases in which the subject cryptocurrencies were seized.[54] A recent January 2018 auction of several blocks of Bitcoin, totaling approximately 3,813 bitcoin in all, is estimated to have generated approximately $44 million in revenue.[55]

III. Recent cases involving cryptocurrency

The cases discussed below address common criminal statutes used in charging cases involving cryptocurrencies, and the investigative tools and forfeiture procedures employed in the seizure of cryptocurrency.

---

[52] *See* FED. R. CRIM. P. 32.2(b)(4).

[53] FED. R. CRIM. P. 32.2(b)(4)(A).

[54] An example of an auction notice published online by the U.S. Marshals Service is available at https://www.usmarshals.gov/assets/2018/bitcoinauction/.

[55] Robin La Quercia, *Crypto Auctions: Where Do Arrested Bitcoins End Up*, BITCOINADVICE.COM (Apr. 29, 2018), https://bitcoinadvice.com/crypto-auctions-where-do-arrested-bitcoins-end-up/.

A. *United States v. Ulbricht* (Silk Road Case)

In February 2015, defendant Ross William Ulbricht was convicted after a trial by jury on seven counts arising from his creation and operation of the Silk Road criminal marketplace on the Darknet, under the username Dread Pirate Roberts (DPR). The Silk Road was used primarily to purchase and sell drugs, false identification documents, and computer hacking software, using Bitcoin as the exclusive form of payment. Between 2011 and 2013, approximately $183 million worth of illegal drugs, as well as other goods and services, were sold using the Silk Road. Ulbricht, acting as DPR, earned millions of dollars in illegal profits from the commissions collected by Silk Road on purchases.

In October 2013, the government arrested Ulbricht, seized the Silk Road servers, and shut down the site.[56] Following his conviction at trial, Ulbricht was sentenced to life in prison and ordered to forfeit $183,961,921. Ulbricht appealed his sentence, which was affirmed in all respects by the United States Court of Appeals for the Second Circuit.[57] The United States Supreme Court denied Ulbricht's petition for writ of certiorari.[58]

Prior to trial, Ulbricht moved to dismiss the indictment. In his motion, he argued, among numerous other claims, that, with respect to Count Four of the indictment, "he cannot have engaged in money laundering because all transactions occurred through the use of Bitcoin and thus there was therefore no legally cognizable 'financial transaction.'"[59] The district court rejected Ulbricht's argument. While finding that the fact that "Bitcoins allow for anonymous transactions does not *ipso facto* mean that those transactions relate to unlawful activities," the very fact that "the system of payment [was] designed specifically to shield the proceeds from third party discovery of their unlawful origin . . . forms the unlawful basis of the money laundering charge."[60]

The court further found that the money laundering statute, 18 U.S.C. § 1956,[61] broadly defines "financial transaction" to include

---

[56] United States v. Ulbricht, 858 F.3d 71, 82–83 (2d Cir. 2017).
[57] *See id.*
[58] Ulbricht v. United States, 138 S. Ct. 2708 (2018).
[59] United States v. Ulbricht, 31 F. Supp. 3d 540, 548 (S.D.N.Y. 2014).
[60] *Id.* at 569.
[61] 18 U.S.C. § 1956.

"all movements of 'funds' by any means, or monetary instruments."[62] Because the term, "funds," is not defined in the statute, the court accorded the ordinary definition of funds as "money, often money for a specific purpose"—that is, "money" as an object used to purchase things.[63] Turning to Bitcoin, the court reasoned that "[b]itcoins can be either used directly to pay for certain things or can act as a medium of exchange and can be converted into a currency which can pay for things[.]" As such, the court concluded:

> The money laundering statute is broad enough to encompass use of Bitcoins in financial transactions. . . . Congress intended to prevent criminals from finding ways to wash the proceeds of criminal activity by transferring proceeds to other similar or different items that store significant value. . . . There is no doubt that if a narcotics transaction was paid for in cash, which was later exchanged for gold, and then converted back to cash, that would constitute a money laundering transaction. . . . [Accordingly,] [o]ne can money launder using Bitcoin.[64]

This holding is significant for forfeiture purposes, since there is broad statutory authority to forfeit any property "involved in" money laundering,[65] which the court here held could include the use (and from that, the forfeiture) of Bitcoin to engage in money laundering.

B. *United States v. Faiella*

In *United States v. Faiella*, the defendants were charged in connection with their operation of an underground market for exchanging Bitcoin for fiat currency on the Silk Road website. Defendant Faiella was specifically charged with operating an unlicensed money transmitting business in violation of 18 U.S.C. § 1960, and conspiring to commit money laundering in violation of 18 U.S.C. § 1956(h). After indictment, Faiella moved to dismiss the section 1960 charge, arguing that Bitcoin does not qualify as "money" under the statute, that operating a Bitcoin exchange does

---

[62] *Ulbricht*, 31 F. Supp. 3d at 570.
[63] *Id.*
[64] *Id.*
[65] *See* 18 U.S.C. §§ 981(a)(1)(A) (civil forfeiture), 982(a)(1) (criminal forfeiture).

not constitute "transmitting" money under the statute, and that he did not qualify as a "money transmitter" under the statute.[66]

Relying on plain meaning definitions, the court first determined that "Bitcoin clearly qualifies as 'money' or 'funds'" that "can be easily purchased in exchange for ordinary currency, acts as a denominator of value, and is used to conduct financial transactions."[67] Second, the court concluded that "Faiella's activities on Silk Road constitute[d] 'transmitting' money under Section 1960[,]" given the allegation that "Faiella received cash deposits from his customers and then, after exchanging them for Bitcoins, transferred those funds to the customers' accounts on Silk Road."[68] Therefore, "in sending his customers' funds to Silk Road, Faiella 'transferred' them to others for a profit."[69] Third, the court held that "Faiella clearly qualifie[d] as a 'money transmitter' for purposes of Section 1960," based on guidance issued by the Financial Crimes Enforcement Network (FinCEN), "specifically clarifying that virtual currency exchangers constitute 'money transmitters' under its regulations."[70] Finally, the court rejected defendant's claim that applying section 1960 to a Bitcoin exchange business would violate the rule of lenity, "constituting such a novel and unanticipated construction of the statute as to operate an *ex post facto* law in violation of the Due Process Clause."[71] The court found that there was "no . . . irreconcilable ambiguity" in the statute's language and structure, legislative history, and motivating policies that would require resort to the rule of lenity.[72]

This case is notable in the forfeiture context, as there is wide statutory authority to forfeit any property "involved in" an 18 U.S.C. § 1960 offense, or any property traceable to such property, which, in this context, could include the Bitcoin exchanged in the illegal money transmitting business.[73]

C. *United States v. 50.44 Bitcoins*

In December 2015, the United States filed a verified complaint for forfeiture against 50.44 bitcoins. The Clerk filed an entry of default on

---

[66] United States v. Faiella, 39 F. Supp. 3d 544, 545 (S.D.N.Y. 2014).
[67] *Id.*
[68] *Id.* at 546.
[69] *Id.*
[70] *Id.*
[71] *Id.* at 547.
[72] *Id.*
[73] *See* 18 U.S.C. §§ 981 (civil forfeiture), 982 (criminal forfeiture).

March 9, 2016, and the United States filed a motion for default judgment on March 10, 2016. No response to the motion was filed. The matter was referred to a magistrate judge for report and recommendations, and the magistrate recommended that the motion for default judgment be granted. In reaching this conclusion, the court assessed whether the government had established that there was a substantial connection between the property—that is, the Bitcoin—and the offense, under 18 U.S.C. § 983(c)(3). The court found that because the business operated by Amanda and Thomas Callahan under the Silk Road username, "JumboMoneyBiscuit," was not registered to transmit money as required by state and federal law, the Callahans violated section 1960. Accordingly, the 50.44 Bitcoins seized from the Callahans constituted property "involved in" a transaction that violated section 1960. Moreover, "[b]ecause the United States ha[d] established a substantial connection between the property to be forfeited and a criminal offense, the 50.44 Bitcoins [we]re subject to forfeiture under 18 U.S.C. § 981 and 983."[74]

The court further found that that the government had complied with Supplemental Rule G's procedural requirements governing the pleading of the civil forfeiture complaint and its notice requirements. Accordingly, "[b]ecause the United States ha[d] complied with the procedural requirements of Rule G and ha[d] met the substantive requirements of 18 U.S.C. § 981, [the court found] that the 50.44 Bitcoins seized from the Callahans [we]re subject to forfeiture."[75]

In June 2016, the district court entered an order agreeing with the magistrate judge's report and recommendation in every respect, entering judgment in favor of the United States against the 50.44 Bitcoins, forfeiting the property to the United States pursuant to 18 U.S.C. § 981(a)(1)(A), and authorizing the Attorney General, or a designee, to seize the forfeited property and take exclusive custody and control of it until its disposal in accordance with the law.[76]

D. *United States v. Vallerius*

In this case, defendant Gal Vallerius moved to suppress certain statements and physical evidence. Vallerius had been arrested for his

[74] United States v. 50.44 Bitcoins, No. CV ELH-15-3692, 2016 WL 3049166, at *2 (D. Md. May 31, 2016).
[75] *Id*. at *3.
[76] *See* Order, United States v. 50.44 Bitcoins (Callahan), No. ELH-15-3692 (D. Md. June 20, 2016).

use of the Darkweb to facilitate international narcotics transactions. Specifically, Vallerius had used the "Dream Market," a website on the Darknet that allowed individuals to create online advertisements offering various narcotics for sale at a set price. Payment for the illicit purchases were made through Bitcoin and other cryptocurrencies, "which add[ed] an additional layer of anonymity to the transaction and conceal[ed] the identities of the accounts from which the cryptocurrency payments originate[d]."[77] Vallerius, as a "senior moderator" on the Dream Market website and using the moniker "OxyMonster," moderated the forums and provided advice to other members about the online drug trade. Vallerius also sold controlled substances to other members using the website, receiving payment for the sales through the use of a Bitcoin "tip jar," or electronic depository. It was through this "tip jar" that law enforcement officials became aware of Vallerius' true identity. Agents tracked several incoming payments and outgoing deposits from the tip jar to various wallets controlled by Vallerius. Agents also compared posts made by OxyMonster on the Dream Market forum with social media accounts used by Vallerius, and determined that the writing style and syntax of OxyMonster's posts on Dream Market matched those written by Vallerius on his social media accounts.[78]

Law enforcement learned that Vallerius would be travelling to the United States from Paris, France, and making entry on August 31, 2017. Upon his arrival at the Atlanta, Georgia airport, Vallerius was "flagged" and pulled aside for secondary inspection by United States Customs and Border Protection (CBP) officers. CBP officers asked Vallerius to open his bags and asked if he was traveling with any electronic devices. He acknowledged that he possessed a laptop computer, a cell phone, and an iPad tablet. The agent asked if the devices were password protected and Vallerius replied in the affirmative. The agent informed him that he would have to provide the passwords to the electronics because the devices were subject to routine inspection at the border. Vallerius complied, providing his passwords, and the electronic devices were removed from his possession. The computer, tablet, and cell phone were transferred to

[77] United States v. Vallerius, No. 17-CR-20648, 2018 WL 2325729 (S.D. Fla. May 1, 2018), report and recommendation adopted, No. 17-20648-CR, 2018 WL 2324059 (S.D. Fla. May 22, 2018).
[78] *Id.* at *1.

the custody of DEA agents, who used the passwords to gain access to the computer and conduct a search of its contents.

On the laptop, the agents located a Bitcoin wallet that they believed could be traced to the OxyMonster account. The agents had the CBP officer request the wallet password from Vallerius, who in response claimed that no password was required for the wallet. Vallerius was then placed under arrest and advised of his *Miranda* rights. Agents then attempted to question him about the contents of the laptop. Vallerius indicated that he wished to consult with an attorney, and the agents thereupon stopped the interview. A search warrant was subsequently obtained to conduct a complete examination of Vallerius' computer.[79]

Vallerius moved to suppress, claiming that initial questioning by the CBP officer, during which the officer requested the computer password and the cell phone personal identification number (PIN) code violated the Fifth Amendment, and that any information obtained as a result of that conversation should be suppressed. In addressing Vallerius's motion, the court first considered whether asking the defendant to provide his computer password and cell phone PIN code, without first *Mirandizing* him, violated the Fifth Amendment. The court observed that, "in the case of those seeking entry to the United States, whether such a person can be considered 'in custody' for purposes of *Miranda* 'should be interpreted in light of the strong government interest in controlling [our nation's] borders.'"[80]

Applying factors set forth by the Eleventh Circuit in *United States v. Moya*,[81] the court concluded that "Vallerius was not in custody at the time he provided his password and PIN codes." He was not placed in handcuffs, no guns were drawn on him when he provided the information, and he never asked to leave the secondary inspection area.[82] The court further found that the border search did not "taint" the subsequent search warrant obtained for the computer.[83] The magistrate recommended that the defendant's motion to suppress be

[79] *Id*. at *2–3.
[80] *Id*. at *3.
[81] United States v. Moya, 74 F.3d 1117 (11th Cir. 1996).
[82] *Vallerius,* 2018 WL 2325729, at *4.
[83] *Id*. at *7.

denied, and the district court adopted the report and recommendation by order filed on May 22, 2018.[84]

This decision is notable, as it may provide authority for asking a subject for not only passwords to access a computer or smart phone, on which evidence of cryptocurrency may be stored, but also for asking for the private key for a cryptocurrency wallet stored therein, at least in the context of a border search.

E. *United States v. 2013 Lamborghini Aventador LP700-4* (AlphaBay Case)

In this in rem civil forfeiture action, the United States filed an ex parte motion for default judgment and final judgment of forfeiture as to several luxury vehicles, bank accounts, real properties, and millions of dollars in various cryptocurrencies. In July 2017, the United States filed a verified first amended forfeiture complaint alleging that between December 2014 and July 2017, the AlphaBay website on the Darknet served as a marketplace for illegal goods such as malware, controlled substances, chemicals, guns, stolen financial information, and counterfeit documents to its users all over the world, including in the Eastern District of California. An individual named Alexandre Cazes founded AlphaBay in 2014 and was its leader through July 4, 2017. He oversaw Alphabay's operations and controlled the profits generated from the operation of the business, receiving tens of millions of dollars in commissions from the illegal transactions facilitated by Alphabay. Alphabay required its users to transact in cryptocurrencies such as Bitcoin, Monero, and Ethereum.[85]

During the investigation stage of the case, between May 2016 and June 2017, United States law enforcement agents made numerous undercover purchases of marijuana, heroin, fentanyl, and methamphetamine; fake identification documents; and an ATM skimmer from AlphaBay vendors. During the course of their investigation, they identified Cazes as "Alpha02" and "Admin," the founder and administrator of AlphaBay. They learned that the personal email address, "Pimp_Alex_91@hotmail.com," was included in the header of AlphaBay's "welcome email" to new users, and in the

---

[84] *See* Order Adopting Magistrate Judge's Report and Recommendation, United States v. Vallerius, Crim. No. 17-20648-CR-Scola, 2018 WL 2324059 (S.D. Fla. May 22, 2018).

[85] United States v. 2013 Lamborghini Aventador LP700-4, No. 1:17-cv-00967-ljo-sko, 2018 WL 3752131 (E.D. Cal. Aug. 8, 2018).

header of AlphaBay's "password recovery process" for users who lost their passwords to the AlphaBay forum. Law enforcement then learned that the email address belonged to Cazes, a Canadian national.[86]

When law enforcement executed a search warrant at Cazes' residence, he was in active communication with one of the AlphaBay data centers about a law enforcement-generated service outage on the site. In addition, passwords to AlphaBay's servers and other evidence was found on Cazes' personal computer linking him to the website. Law enforcement also determined that Cazes owned and controlled a front company called EBX Technologies, which he used to "justify his banking activity and substantial cryptocurrency holdings."[87]

In June 2017, a warrant was issued for Cazes' arrest based upon a 16-count indictment[88] charging him with, among other things, RICO conspiracy, drug conspiracy, conspiracy to commit identify theft and access device fraud, and conspiracy to commit money laundering. The indictment also sought to forfeit all assets connected to the AlphaBay criminal organization. Additionally, in June 2017, a federal judge in the United States found probable cause to issue seizure warrants for a luxury vehicle and eleven bank and cryptocurrency exchange accounts traceable to unlawful proceeds generated from AlphaBay. Law enforcement had traced Bitcoin transactions conducted in AlphaBay to digital currency accounts, bank accounts, and other assets owned by Cazes and his wife.[89] In Thailand, where Cazes lived with his wife, law enforcement also identified numerous bank and digital exchange accounts tied to Cazes containing illicit proceeds from AlphaBay operations, which digital exchange accounts Cazes used to liquidate his cryptocurrency (usually Bitcoin) so that he could spend the proceeds in Thailand and other countries on expensive cars, real estate holdings, and other assets.[90]

---

[86] *Id*. at *4.
[87] *Id*. at *4–5.
[88] *Id*. at *4 (dismissing all 16 counts of the indictment in April 2018, following Cazes' death; the civil forfeiture action survived, as the government may still seek civil forfeiture of the property of defendants who have died). *See* United States v. Real Property at 40 Clark Road, 52 F. Supp. 2d 254, 265 (D. Mass. 1999) (explaining that defendant's death during the pendency of the criminal forfeiture proceedings made civil forfeiture necessary).
[89] *Lamborghini*, 2018 WL 3752131 at *5.
[90] *Id.*

On July 5, 2017, the Royal Thai Police, with assistance from the FBI and the DEA, executed an arrest warrant for Cazes, as well as a search warrant at his primary residence in Bangkok, Thailand. At the time of his arrest, his laptop was open and in an unencrypted state, and logged into the AlphaBay forums and the server that hosted the AlphaBay website under the username, "Admin." Because his computer was unlocked and unencrypted, law enforcement was able to search Cazes' computer and found several open text files with passwords/passkeys for the AlphaBay website, all of the AlphaBay servers, and other online identities associated with AlphaBay. As a result, law enforcement was able to seize all of the information and cryptocurrency on the AlphaBay servers. Additionally, law enforcement found a document containing wallet addresses with the private keys written next them, which allowed law enforcement to transfer the cryptocurrency in each wallet to a secure government-controlled wallet address. In total, from Cazes' wallets and computer, agents assumed control of approximately $8,800,000 in Bitcoin, Ethereum, Moreno, and Zcash. Law enforcement also identified and seized certain servers that hosted AlphaBay cryptocurrency wallets, some unencrypted and others encrypted. In addition, law enforcement seized information and cryptocurrency from IP addresses containing AlphaBay's entire universe of cryptocurrency.[91]

The United States filed its civil forfeiture complaint on July 19, 2017, and an amended forfeiture complaint on July 26, 2017. Based on the allegations in the amended complaint, the Clerk of Court issued a warrant for arrest of articles in rem for the defendant assets. In August 2017, the court issued an order allowing public notice of the forfeiture action for 30 consecutive days on the official government forfeiture website, www.forfeiture.gov. Publication began on September 27, 2017, and ran for at least 30 consecutive days, consistent with Supplemental Rule G(4)(a). The United States also provided notice to various potential claimants who might have had an interest in the defendant properties. In addition, the government coordinated with the governments of Thailand, Antigua, and Cyprus to post copies of the notice of the forfeiture complaint on the real properties purchased by Cazes in those countries. On November 14, 2017, the Clerk of Court entered default against all of the known

[91] *Id*. at *5–7.

claimants, and the United States filed an ex parte motion for default judgment and final judgment of forfeiture on June 1, 2018.[92]

In determining whether the government's motion for default judgment should be granted, the court first determined the sufficiency of the forfeiture complaint. With respect to the cryptocurrency, specifically, the court observed that the complaint alleged that "[f]ederal agents traced Bitcoin transactions originating with AlphaBay to digital currency accounts, and ultimately bank accounts and other tangible assets held by Cazes and his wife." The complaint further alleged that "Cazes concealed and disguised the illicit source of the funds by commingling the criminal proceeds in digital currency exchange accounts and bank accounts controlled by Cazes and his wife, and using an automated mixing and tumbling procedure designed to conceal the source of the criminal funds when converting Bitcoin (and other cryptocurrencies) to currency." The complaint also alleged that at the time of his arrest, Cazes' laptop was logged into the server hosting the AlphaBay website and law enforcement identified passwords and passkeys for, among other things, the cryptocurrency wallets contained on each server. Law enforcement also, the complaint alleged, found a document listing, among other things, Cazes' cryptocurrency holdings. Given the absence of asserted interests in the defendant assets, the court "therefore [found] that the facts, as alleged, provide[d] a sufficient connection between the Defendant Assets and illegal money laundering, racketeering, fraud, and drug activity, to support forfeiture."[93]

The court also found that the government had satisfied Supplemental Rule G's notice requirements, as to the defendant properties, that the time to file a claim had expired, and that therefore the Clerk of Court properly had entered defaults against the potential claimants. The magistrate concluded, therefore, that the government had met the procedural requirements for civil in rem forfeiture actions set forth in 18 U.S.C. §§ 983 and 985, and recommended the granting of the government's ex parte motion for default judgment, and the entry of a final judgment of forfeiture to be submitted by the government.[94] The district court's decision as to whether to adopt the findings and recommendations of the magistrate court are still pending as of the writing of this article.

---

[92] *Id*. at *9.
[93] *Id*. at *11–12.
[94] *Id*. at *14.

This case exemplifies the tremendous success that can be achieved through careful pre-seizure investigation and planning, utilizing investigative techniques aimed to identify "dirty" cryptocurrency transactions and Darknet activity, and tracing those transactions to a specific individual.

IV. Conclusion

As demonstrated above, asset forfeiture plays a critical role in the identification, seizure, preservation, and liquidation of cryptocurrency that is used to engage in criminal activity. Asset forfeiture allows law enforcement to take "tainted" cryptocurrency out of the hands of wrongdoers who exploit the anonymity of cryptocurrency to operate and profit from criminal enterprises.

About the Author

Shirley U. Emehelu is Chief of the Asset Recovery and Money Laundering Unit (ARMLU) at the United States Attorney's Office for the District of New Jersey (DNJ), where she has been an Assistant United States Attorney in the Newark office since 2010. As Chief of ARMLU, Ms. Emehelu supervises the unit's Asset Forfeiture, Money Laundering, and Financial Litigation Assistant United States Attorneys and support staff. Prior to becoming Chief of ARMLU, Ms. Emehelu was an Assistant United States Attorney in DNJ's Economic Crimes Unit. Following her tenure in the Economic Crimes Unit, Ms. Emehelu was in the Special Prosecutions Division of the United States Attorney's Office, where she investigated and prosecuted public corruption cases, many of which involved financial fraud.

Prior to joining the United States Attorney's Office, Ms. Emehelu worked as a litigation associate in the New York office of a global law firm, where her practice focused on internal corporate investigations, federal grand jury and regulatory investigations, corporate compliance, and complex commercial litigation.

Additionally, Ms. Emehelu served as an Adjunct Professor at Montclair State University in the fall of 2014, where she taught White Collar Crime in the University's Justice Studies department. Ms. Emehelu clerked for the Honorable James R. Spencer in the Eastern District of Virginia. She received her J.D. from Yale Law School, where she was an Editor for the Yale Law Journal and a Member of the Journal's Admissions Committee, and her bachelor's degree in Political Science, with distinction, from Yale University.