Keeping a Lid on the Crypt: Protecting Taxpayers' Fifth Amendment Rights to Not Produce Incriminating Crypto Records

By Kevin F. Sweeney*

Kevin F. Sweeney examines how a segment of cryptocurrency owners are using its pseudo-anonymous features to conceal virtual assets and income from the IRS and the use of the Taxpayer's Fifth Amendment rights to not produce incriminating crypto records.

KEVIN F. SWEENEY is a former federal tax prosecutor with the U.S. Department of Justice, Tax Division.

Similar to the way U.S. taxpayers historically used Swiss bank secrecy laws to conceal assets and income in foreign bank accounts, a segment of cryptocurrency ("crypto") owners are now using its pseudo-anonymous features to conceal virtual assets and income from the Internal Revenue Service ("IRS" or "Service") and the U.S. Department of Justice ("DOJ") (collectively the "Government"). Recognizing this issue, the Government has begun a tax enforcement campaign to crack down on unreported crypto. Accordingly, in the coming months and years, taxpayers and their practitioners may soon find themselves in the midst of crypto-related civil audits and criminal investigations. In these cases, noncompliant taxpayers are likely to face the difficult decision of whether to voluntarily comply with summonses and subpoenas for incriminating crypto records or invoke their Fifth Amendment act of production privilege. Although assertions of this privilege have been largely unsuccessful in recent years in the context of foreign bank account cases, crypto tax cases present new and promising applications of this longstanding doctrine for taxpayers. With the assistance of an experienced criminal tax attorney, taxpayers may be able to repel Government efforts to compel the production of such records and, in turn, avoid otherwise inevitable criminal indictments and prosecutions.

Background

For decades, wealthy Americans passed up the convenience of local banks for the financial anonymity of Swiss bank accounts located half a world away. Through a

choreographed dance of bank secrecy laws, hold mail, numbered accounts, offshore structures, and insurance wrappers, Swiss banks built an industry around assisting U.S. and other clients to conceal assets and income. Switzerland was not the only jurisdiction that offered these privacy protections and banking services, but few others could compete with its reputation for stability and predictability.

In the late 2000s, the landscape of the offshore banking world started to change, beginning with Swiss Bank UBS AG's ("UBS") receipt of an IRS John Doe Summons and its subsequent Deferred Prosecution Agreement ("DPA") with DOJ. As part of this DPA, UBS facilitated the exchange of undeclared U.S. bank account information to U.S. tax authorities. Over the next decade, over 80 Swiss and other international banks would likewise turn over the figurative keys to billions of dollars of sensitive assets entrusted to them by wealthy American clients.

Today, Americans seeking financial anonymity are unlikely to find it in offshore bank accounts. Many believe that crypto is the new Swiss bank account. With a few clicks of a mouse, taxpayers can now hold and transfer virtual coins pseudo-anonymously without the need for bankers or third-party intermediaries.

Understandably, the Government is concerned that people are utilizing crypto to conceal assets and income from the Service. At a recent Federal Bar Association meeting in Washington, D.C., the IRS Chief of Criminal Investigation noted that crypto is an immediate concern and area of focus for IRS criminal investigators.[1] Moreover, the Service's Large Business & International ("LB&I") Division has announced a campaign that focuses on unreported crypto income.[2] These statements are consistent with recent tax enforcement actions like the Service's issuance of a John Doe Summons to the U.S.-based crypto exchange Coinbase. Similar to the role that the UBS John Doe summons played in its eventual undeclared offshore bank account campaign, the Coinbase John Doe summons is likely just the tip of the Government's spear in crypto tax enforcement.

The Government's ability to acquire records of unreported crypto assets and income will undoubtedly be a lynchpin in future prosecutions. As it ramps up its tax enforcement campaign, practitioners are likely to encounter noncompliant taxpayers faced with IRS summonses, grand jury subpoenas, and court orders pursuant to The All Writs Act compelling incriminating crypto records. While there is no Fifth Amendment privilege to refuse the production of such records on the ground that they are inherently incriminating,[3] the act of producing such records may be protected in some circumstances.

Over the last decade, much has been written about the Fifth Amendment act of production doctrine in the context of offshore tax evasion cases. In recent years, the Government has been immensely successful in compelling the production of incriminating foreign bank account records by establishing the applicability of exceptions like the collective entity, required records, and/or foregone conclusion doctrines. However, due to the unique manner in which virtual coins are held and transferred, it will face different issues and untested applications of these long-standing principles with crypto. Given the Government's focus on virtual currency, practitioners would be well served to consider these differences and the likely effect they will have on their clients' ability to successfully invoke the Fifth Amendment act of production privilege.

1. Act of Production Doctrine

The Fifth Amendment generally protects individuals against government compulsion of incriminating communications. It states that "[n]o person … shall be compelled in any criminal case to be a witness against himself."[4] However, not every compelled communication is protected. The Fifth Amendment "applies only when the accused is compelled to make a testimonial communication…"[5] For a communication to be testimonial, it must "explicitly or implicitly … relate a factual assertion or disclose information."[6]

The Supreme Court has found that, in some instances, the Fifth Amendment extends to the act of producing documents in response to a summons or subpoena.[7] This legal principle is known as the act of production doctrine. The Court has reasoned that "[t]he act of producing evidence in response to a subpoena [or other means of compulsion] … has communicative aspects of its own, wholly aside from the contents of the papers produced."[8] To that end, the compulsion of documentary evidence may "tacitly concede … the existence of the documents demanded and their possession and control by the [defendant]."[9] As the Third Circuit put it, by "producing documents, one acknowledges that the documents exist, admits that the documents are in one's custody, and concedes that the documents are those that the [Government] requests."[10]

In order to advise crypto holders on Fifth Amendment act of production issues, practitioners must understand how crypto is held and transferred. Since crypto coins are virtual in nature, there is no physical object to possess. Instead, crypto owners hold the cryptographic keys of their coins. These keys are generally stored in digital wallets. For each coin in a non-custodial wallet,[11] the taxpayer holds one public key and one secret private key in the form of lengthy number and letter combinations.

To transfer crypto coins, the holder must identify and communicate to his or her wallet the wallet address of the

intended recipient. Once the transaction is submitted, it must be validated by a network of third-parties called miners, who attempt to match the secret private key of the sender with the public key recorded in a public ledger called the blockchain. Completed transactions are signified through the generation of a transaction ID, their recording in the blockchain, balance adjustments to the wallets of the sender and recipient, and the transfer of possession of the coin's private key from the sender to the recipient.[12] While blockchain transactions are publicly traceable, the identities of blockchain transaction participants are generally not. This combination of publicly transparent transactional data and secret identifying information fosters trust in the legitimacy of crypto transactions while maintaining a degree of anonymity for transaction participants.

It is common for users to hold and transfer coins among multiple wallets. Crypto is most often bought and sold using online exchanges that require, at a minimum, the temporary use of an exchange-based wallet.[13] However, not all exchanges trade the same crypto coins and, even when they do, prices may differ. Consequently, users often buy and sell coins on multiple exchanges. Additionally, many users don't trust exchange-based wallets to store and secure their private keys.[14] Accordingly, they transfer to, and store coins in, other wallets when they are not conducting transactions. Some insist on the security of paper wallets and tamper-proof electronic hardware devices while others prefer wallets that are accessible on Internet browsers and personal electronic devices.

The Government playbook for crypto tax enforcement appears to be focused on the compulsion and cooperation of custodial exchanges.[15] Earlier this year, the Service was successful in compelling Coinbase to provide wallet information concerning over 13,000 U.S. customers.[16] More recently, Bitfinex, a British Virgin Islands exchange, indicated that it would be indirectly providing wallet information for certain customers to the Service pursuant to FATCA.[17] Noncompliant taxpayers that use custodial exchange-based wallets ("custodial wallets") to hold and transact crypto are easy targets for the Government. Rather than particular coins, custodial exchanges generally permit users to store and transact fungible crypto value corresponding to particular coins owned by the exchange.[18] These wallet transactions are recorded off-blockchain in internal records. This makes transaction participants identifiable in the records of the exchange.

Once in possession of custodial wallet information, the Government is likely to reconcile it against IRS taxpayer records to develop targets for audits and criminal investigations. If targeted by the Service, a taxpayer can expect to receive information document requests ("IDRs"), summonses, and/or subpoenas for crypto wallet records. For taxpayers with significant unreported crypto income or a paper trail indicating active concealment from the Service, compliance with such Government requests is likely to put them at serious risk of criminal prosecution.

Generally speaking, the Government only brings criminal tax prosecutions in cases where there is a substantial unreported tax liability.[19] The Service has determined that crypto is treated as property for tax purposes.[20] Rather than creating crypto-specific rules, it has declared that general tax rules concerning property transactions will apply.[21] Consistent with these principles, crypto that is paid to taxpayers as compensation for services such as mining will generally be taxed as ordinary income while crypto held for investment purposes will typically be treated as a capital asset.[22]

In criminal cases, the Government bears the formal and/or informal burden of proving a tax liability.[23] For example, it must prove a tax due and owing for Code Sec. 7201 counts, the materiality of false items for Code Sec. 7206(1) counts, and the extent of the tax loss caused by relevant conduct at sentencing.[24] With respect to unreported crypto held as a capital asset, the Government must prove that the sales price exceeded the cost basis in order to establish a tax liability.[25] General tax principles require that, in computing cost basis, it use the specific identification method.[26]

The Government is likely to encounter several issues in attempting to prove the cost basis of coin sales.[27] First, with respect to custodial wallets, the fungible nature of crypto held and transacted is not conducive to the specific identification method.[28] Second, this method requires the Government to trace the cost basis of particular crypto coins back to the original purchase date.[29] When all of a taxpayer's crypto is purchased, held, and sold on one exchange, this may not be too difficult. However, where a taxpayer holds crypto in multiple wallets and transfers coins among them, one wallet may not be enough to calculate cost basis. This is because, when coins are transferred among multiple taxpayer wallets before being sold from one of them, the purchase price cannot be learned from analyzing the wallet that sold the coins alone.[30] In these types of cases, the Government may need to obtain the records of most or all of the taxpayer's wallets and then trace the transfers among them to find the original purchase dates and prices of the coins sold.[31]

To the extent unreported crypto sold by a taxpayer is fungible and/or wallet records necessary to trace particular coins cannot be obtained by the Government, it will be difficult if not impossible for it to compute cost basis using the specific identification method. In a civil examination, where the burden is on the taxpayer, the Service has deemed the cost basis of property to be zero in situations where proof of cost basis cannot be established

using a legally permissible method.[32] Following converse logic, one could argue that, in a criminal case where cost basis cannot be reliably computed using the only legally authorized method—specific identification, courts should deem the cost basis of a particular coin sale to be the highest purchased like-amount when all relevant purchase prices are known to the Government. Moreover, when all relevant purchase prices are not known to the government, it should be deemed to be 100 percent of the sales price of each coin sold. Practically speaking, any other method used by the Government would be susceptible to a cross-examination that highlights all of the other more taxpayer-friendly ways it could have attempted to accomplish the difficult if not impossible task of computing cost basis using the specific identification method. In addition to the problems that these issues create for the government in establishing the existence of a tax liability, confusion surrounding the proper way of computing crypto cost basis in these circumstances is likely to cut against taxpayer willfulness.

By voluntarily providing wallet records to the Government in response to an IRS summons or grand jury subpoena, the taxpayer could be delivering him or herself to criminal investigators and prosecutors on a silver platter. Compliance may concede the existence of wallet records not otherwise known to the Government as well as the taxpayer's custody of these records. Moreover, the documents themselves could be highly probative of unreported income, cost basis, taxpayer concealment, and can assist the Government in developing leads for other wallets and unreported income. On the other hand, an unsuccessful assertion of Fifth Amendment privilege during a civil audit will increase the likelihood of a criminal referral and can result in the Service making an assessment based on a reduced or zero cost basis.

Based on what is at stake, it is imperative that an attorney experienced in criminal tax matters be consulted as soon as the taxpayer or his or her practitioner learns that Government officials are inquiring into matters directly or indirectly related to unreported crypto. This is even more important when the representative is a non-attorney because the Code Sec. 7525 tax practitioner privilege will not protect communications with the taxpayer in the event the case turns criminal.[33] Once the proper representative team is in place, it must assess, among other items, whether the compelled records are testimonial and personally incriminating to the taxpayer as well as whether the Government is likely to discover them anyway so as to make an assertion of privilege futile. To this end, they will need to determine whether any exceptions to the Fifth Amendment act of production doctrine are likely to preclude a successful assertion of privilege.

2. Collective Entity Doctrine

The first exception to the Fifth Amendment act of production doctrine is known as the collective entity doctrine. It is based on the fundamental principle that, unlike individuals, legal entities do not have Fifth Amendment rights.[34] It was formed by a line of Supreme Court cases starting with *Wilson* and continuing through *R. Braswell* that, as a whole, concluded that a representative of a legal entity cannot assert his or her own personal privilege to avoid turning over an entity's documents.[35] This is the case even if the documents tend to incriminate the representative personally.[36] The collective entity doctrine has been found to apply to the records of most businesses formed as non-sole proprietorships to include corporations, partnerships, trusts, LLCs, and even single member LLCs ("legal entity businesses").[37]

In some cases in which a taxpayer operates a crypto business as a separate legal entity, the application of the collective entity doctrine is straightforward because the line between personal and legal entity business records is defined. In other cases, the issues are not so clear-cut. As taxpayers sometimes do with bank accounts, many crypto users commingle coins received from legal entity businesses engaged in mining or trading with personal coins in their crypto wallets.[38] Moreover, based on the lackadaisical know-your-customer standards at many exchanges, taxpayers sometimes open up wallets used partially and/or primarily for legal entity businesses in either their own name or a fictitious one.

Based on the developing nature of crypto tax law, practitioners and their taxpayer clients often face new and untested issues for which they must take tax positions. For issues involving the classification of crypto as either personal or legal entity business assets, these positions may have Fifth Amendment implications. Characterization becomes particularly important when assisting clients with amended and/or current year tax returns that come due during an audit or criminal investigation. Once a return is filed taking the position that crypto related assets, income, or expenses belong to a particular legal entity business, it could foreclose future arguments that the underlying records are personal in nature and, in turn, preclude the taxpayer from successfully invoking his or her Fifth Amendment privilege as to the act of producing them. For instance, to the extent that a return position is taken that crypto coins earned mining became part of the inventory of the taxpayer's single member LLC business, this position could be used against the taxpayer by the Government if the taxpayer later asserts the Fifth Amendment with respect to the production of the wallets holding these coins.

In determining whether documents are personal or legal entity business records, courts employ a functional test that examines the documents' nature, function, and use.[39] With respect to commingled records, courts are disinclined to permit a taxpayer to avoid production altogether on Fifth Amendment grounds.[40] To the contrary, records that contain a significant mixture will likely be considered legal entity business records not protected by privilege.[41] Nonetheless, with respect to situations where coins held and transacted for personal use are readily severable from legal entity business coins in the same wallet, there is limited precedent for permitting those records to be "culled so as to delete or excise purely private notations from [the] corporate record, or corporate materials mingled with private [ones]."[42]

3. Required Records Doctrine

Another exception to the Fifth Amendment act of production privilege is the required records doctrine. This doctrine precludes compelled taxpayers whose records are required to be maintained by law from validly invoking their Fifth Amendment privilege against self-incrimination.[43] It was first set forth by the Supreme Court in *Shapiro* and expounded upon in *J. Marchetti*[44] and *A.M. Grosso.*[45] For the required records doctrine to apply, the following three requirements must be met:

> First, the purposes of the Government's inquiry must be essentially regulatory, rather than criminal. Second, the records must contain the type of information that the regulated party would ordinarily keep. Third, the records "must have assumed 'public aspects' which render them at least analogous to public documents."[46]

Compelled domestic crypto wallet records are not likely to fall within the required records doctrine. In *H.V. Porter*,[47] the Seventh Circuit examined whether the required records doctrine was applicable to records that taxpayers are mandated to maintain for tax return substantiation purposes pursuant to Section 6001 of the Internal Revenue Code. The Court rejected the Government's argument for application of the required records doctrine. In so doing, it reasoned that, contrary to the *Shapiro* case, taxpayers are not required to keep such records as an ongoing condition of operating under a comprehensive regulatory scheme. Additionally, it stressed that "the very nature of the limited taxpayer-government relationship is … insufficient to imbue the taxpayer's cancelled checks and deposit slips with 'public aspects' as required under *Shapiro*."[48]

Although tax forms and returns reporting crypto income and receipts may fall within the required records doctrine, courts disagree about this issue.[49] Consequently, taxpayers and their attorneys should be mindful of the precedent in their respective circuits. In unreported crypto tax cases, the Government is most likely to be interested in Forms 1099-K and 1099-MISC reporting crypto receipts. Although the Government will likely already possess information about these tax forms from IRS databases, it is possible that they were never received by the taxpayer. By providing Forms 1099-K and 1099-MISC in response to a summons or subpoena, the taxpayer could concede receipt, and thus admit knowledge of unreported crypto receipts.

Whether compelled foreign crypto wallet records fall within the required records doctrine probably depends, in large part, on whether they constitute foreign financial accounts under the Bank Secrecy Act ("BSA"). Over the last decade, every circuit that has examined the issue of whether a foreign financial account that must be maintained under the BSA is a required record has concluded that it is.[50] In one of the seminal cases, *In re Grand Jury Investigation M.H.*, the Ninth Circuit examined whether the taxpayer could invoke the act of production doctrine to avoid producing Swiss bank account records compelled by a grand jury subpoena.[51] It found that the required records doctrine applied and compelled the taxpayer to produce the documents.[52] In determining whether the applicable requirements were met, the Court reasoned that there is nothing inherently illegal in having an offshore foreign financial account.[53] Additionally, it found that the records were of the type that bank customers would customarily keep because they must report account information to the IRS every year as part of the Government's regulation of offshore banking activity and because they need the information to access their foreign bank accounts.[54] Finally, the Ninth Circuit determined that, since the requisite personal information was being compelled in furtherance of a valid offshore banking regulatory scheme, the information assumed a public aspect.[55]

While there is no longer any question that the required records doctrine applies to summonses and subpoenas for foreign financial accounts that must be maintained pursuant to the BSA, the question of whether a foreign wallet is a foreign financial account under the BSA is less clear. Under the BSA, U.S. persons with a financial interest in, or authority over bank accounts, securities accounts, or other financial accounts located in foreign countries[56] must file a FinCEN Form 114 (more commonly known as an "FBAR") if the aggregate value of these accounts exceeds $10,000 at any time during the calendar year.[57] Additionally, to the extent there is an FBAR requirement, taxpayers must also maintain records of their foreign bank, securities, and other financial accounts for five years and make them "available for inspection as authorized by law."[58]

The applicability of the required records doctrine is likely to specifically depend on whether the particular crypto wallet being compelled is considered an "other financial account" under the BSA. The BSA defines this term in several ways including as an "account with a person in the business of accepting deposits as a financial agency."[59] It further defines financial agency, in part, as a "person acting outside the United States for a person … as a financial institution…"[60] Financial institution is, in turn, defined to include money transmitters. For crypto wallet purposes, FinCEN has found that a "money transmitter" is, in part, a business that: (1) exchanges crypto for real currency, funds, or other virtual currency; and (2) accepts and transmits crypto.[61] In an effort to clarify the term "other financial account," the Internal Revenue Manual ("IRM") specifies several types of accounts that are generally not considered other financial accounts.[62] One such unreportable account is a safe deposit box.[63] However, this clarifying provision is not without exception. The IRM notes that "a reportable account may exist where the financial institution providing the safety deposit box has access to the contents and can dispose of them upon instruction from, or prearrangement with, the person."[64]

All foreign crypto wallets are not created equal. There are three general types of crypto wallets: 1) stand-alone web-based ("personal wallets"), 2) non-custodial exchange-based ("peer-to-peer wallets"), and 3) custodial wallets.[65] Personal wallets allow users to hold particular coins on various personal devices and to transfer them in peer-to-peer transactions recorded in the blockchain. Peer-to-peer wallets similarly permit users to hold particular coins and to transfer them in peer-to-peer transactions recorded in the blockchain, but are provided by virtual peer-to-peer marketplaces that facilitate these transactions.[66] Custodial wallets permit users to hold fungible crypto value, sometimes convert it into and out of fiat, and buy and sell it through its virtual marketplace in off-blockchain transactions.[67] Practitioners should take the time to learn about the types of foreign wallets used by their clients.

Personal wallets provided by foreign companies are unlikely to be considered "other financial accounts" for several reasons. First, personal wallet providers are likely not money transmitters because they do not technically accept and transmit crypto. Such providers never formally accept possession of a user's coins. Instead, the private keys received by the wallet belong to and remain in the continuous and exclusive possession of its users. The transfers of coins in and out of these wallets are conducted by the users themselves in peer-to-peer transactions. In reality, the wallet is nothing more than software that provides users with coin storage and transfer capabilities. In a recent ruling, FinCEN examined whether the production and distribution of software designed to facilitate the sale of crypto constitutes acceptance and transmission. FinCEN ruled that the software production and distribution "*in and of itself,* does not constitute acceptance and transmission of value, even if the purpose of the software is to facilitate the sale of virtual currency."[68] Second, the fact that personal wallets do not directly exchange crypto for real currency, funds, or other crypto also likely precludes their providers from qualifying as money transmitters. While a personal wallet user may agree to accept or transmit real currency, funds, or other crypto in some other manner in exchange for a crypto transfer, this is typically not facilitated by the wallet itself. Finally, personal wallets are analogous to safe deposit boxes, which the Service does not consider "other financial accounts." Much like a safe deposit box could store particular gold bars, personal wallets allow a user to securely store copies of private keys for particular coins. Absent the user giving the wallet provider his or her encryption password and permission to dispose of the crypto inside, the wallet provider should not be able to legally do so. Consequently, taxpayers with personal wallets provided by non-U.S. companies are likely not subject to the FBAR reporting and record maintenance requirements of the BSA and, in turn, compelled requests for these records should not fall within the required records doctrine.

Peer-to-peer wallets operated by foreign providers are also unlikely to be considered "other financial accounts." These operate like personal wallets but are provided by peer-to-peer exchanges. In many instances, these exchanges provide an additional layer of security for peer-to-peer transactions such as the implementation of multi-signature ("multi-sig") technology. Utilizing this technology, they act as third-party authenticators and arbiters of coin transactions. In reality, peer-to-peer exchanges are nothing more than providers of virtual marketplace, key storage, and coin transfer software. Consequently, providers of peer-to-peer wallets are also not likely to be considered money transmitters. Moreover, like personal wallet providers, peer-to-peer exchanges generally cannot legally access private keys or dispose of the particular coins in a wallet without some form of user authorization. As a result, wallets provided by peer-to-peer exchanges are analogous to a safe deposit box. Taken together, taxpayers with peer-to-peer wallets outside the United States are also likely not subject to the FBAR reporting and record maintenance requirements of the BSA and, in turn, compelled requests for these records should not fall within the required records doctrine.

Although there is no judicial precedent or ruling on the issue, it is possible that the Government will treat

custodial wallets operated by foreign providers as "other financial accounts" covered by the BSA. These wallets do not generally permit users to hold particular coins and corresponding private keys. Instead, when users transfer coins into these wallets, the exchange takes possession of them and their corresponding private keys and credits the wallet with their fungible value. Most also allow users to purchase with and convert coins into fiat. Transactions among users occur off blockchain using the fungible values in their wallets. While the exchange may transfer particular coins to the user with corresponding private keys upon him or her cashing out, these will almost never be the same ones initially deposited. FinCEN has indicated that it generally considers custodial exchanges to be money transmitters.[69] Moreover, wallets provided by these exchanges are arguably dissimilar to safe deposit boxes because they do not hold users' particular coins.[70] As possible "other financial accounts," taxpayers with a financial interest in one or more custodial wallets with an aggregate value over $10,000 may be subject to FBAR reporting and records maintenance requirements for a period of five years under the BSA.[71]

Even if custodial wallets are ultimately deemed to be "other financial accounts" under the BSA, it does not necessarily mean that taxpayers who hold such records are subject to the required records doctrine. While the records maintenance requirements of the BSA have consistently been found to meet all three required prongs, it is equally important that courts and litigants not lose sight of the reasons the doctrine exists in the first place. Several courts have noted that:

> One of the rationales, if not the main rationale, behind the required records doctrine is that the government or a regulatory agency should have the means, over an assertion of the Fifth Amendment Privilege, to inspect the records it requires an individual to keep *as a condition of voluntarily participating in that regulated activity*.[72]

In the various cases concluding that the required records doctrine applies to compelled foreign bank account records, there was no dispute concerning whether the particular records at issue were categorically required to be maintained pursuant to the BSA as a matter of law. After all, foreign bank accounts are specifically included in the definition of foreign financial accounts under the BSA. However, foreign custodial crypto wallets are not specifically included in the BSA definition and there is a lack of certainty concerning whether they qualify as "other financial accounts."

Given this uncertainty, in addition to evaluating whether the three prongs of the required records doctrine test have been met, courts may and should also examine whether, as a matter of law, individuals who open foreign crypto wallets can *voluntary participate* in the foreign financial account maintenance rules of the BSA. While the term "voluntary participation" is largely undefined in this context, the Seventh Circuit has loosely indicated that an individual voluntarily participates in a regulated activity when he or she "enters upon a regulated activity knowing that the maintenance of extensive records available for inspection by the regulatory agency is one of the conditions of engaging in the activity."[73] Following this logic, it seems that, for the three prong required records doctrine test to even be relevant in the first place, there must be reason for taxpayers to know that the maintenance of wallet records available for inspection by the Service and/or FinCEN pursuant to the BSA is a condition of their decision to store and transfer for value cryptographic keys using wallets provided by non-U.S. custodial exchanges.[74] Until there is clear guidance regarding the application of the BSA to foreign custodial wallets, it may be difficult for the Government to establish that foreign wallet holders *voluntarily* participate in an activity regulated by the BSA.[75] The question of whether a custodial wallet provided by a non-U.S. company is subject to BSA FBAR reporting and record maintenance requirements is unsettled[76] and far from obvious.[77] After all, the crypto coins they hold are virtual in nature and, thus, do not exist in any one place. For taxpayers desiring an answer, there is no crypto specific case law, statute, regulation, or agency guidance that can be relied upon. It is even unclear if the agency proponents, FinCEN and the IRS, have themselves reached a consensus on this question.[78] Given the uncertainty concerning whether it is, in fact, a requirement for taxpayers to maintain records of foreign crypto wallets under the BSA, a preclusion of Fifth Amendment privilege on required records grounds would arguably render the doctrine a misnomer. As the Fifth Circuit has stated concerning unsettled tax questions, "a criminal proceeding … is an inappropriate vehicle for pioneering interpretations of tax law."[79]

In cases where the DOJ believes the required records doctrine applies, it typically issues a special type of subpoena for documents commonly referred to as a Title 31 subpoena. In foreign account cases, these subpoenas typically limit the scope of the requested documents to any and all records required to be maintained pursuant to the FBAR and corresponding records maintenance requirements of the BSA. However, such subpoenas generally do not provide an exhaustive list of the types of foreign accounts that are subject to these requirements.

As described above, while the BSA clearly specifies that foreign bank and securities accounts are subject to these requirements, the issue of whether a foreign crypto wallet constitutes an "other financial account" is not enumerated in any statute, regulation, or court opinion. Given the lack of guidance, a Title 31 subpoena is likely to place the burden on the taxpayer to determine whether foreign crypto wallet records constitute "other financial accounts," and in turn, whether such records are required to be produced pursuant to both the BSA and the subpoena. This puts taxpayers in a difficult predicament. Given the uncertainty, if the taxpayer produces foreign crypto wallet records, he or she may unnecessarily provide incriminating documents to the government that would otherwise be protected by the Fifth Amendment. On the other hand, if the taxpayer treats the records as not covered by the subpoena, he or she risks a contempt violation. Moreover, it is difficult for the taxpayer to broach the issue with the government without providing a lead concerning the foreign crypto wallet(s) at issue.

In addition to arguing that the required records doctrine is generally inapplicable to a Title 31 subpoena for foreign crypto tax records, taxpayers and their representatives should consider moving to quash and/or modify it based on its language. As the Seventh Circuit has noted:

> The authority of a grand jury to inquire into violations of criminal law through the use of subpoenas *duces tecum* is necessarily broad, and is generally limited only by the requirement that the evidence to be produced cover a reasonable period of time, is relevant to the investigation, and *is identified with reasonable particularity.*[80]

To this end, Rule 17(c) of the Federal Rules of Criminal Procedure provides, in part, that "the court on motion made promptly may quash or modify the subpoena if compliance would be unreasonable or oppressive." In *In re Grand Jury Investigation*, the Eastern District of Wisconsin examined a motion to quash and/or modify a subpoena that was alleged to lack particularity to the point that the recipient could not "reasonably understand what [was] sought." The court found that the subpoena lacked sufficient particularity and quashed it. Moreover, in *In re Grand Jury Subpoena Duces Tecum Served on Allied Auto Sales, Inc.*,[81] the District of Rhode Island examined a motion to quash and/or modify a subpoena issued for documents subject to the required records doctrine. In that case, even though the court found that the required records doctrine generally precluded a valid assertion of the Fifth Amendment in that case, it indicated that a "request which commands a witness who may also be a grand jury target to construe a subpoena in [a manner] involving the discretionary mental processes of the witness" may nonetheless "run afoul of Fifth Amendment privilege."

Absent the government specifying in the subpoena precisely what records it deems to be and not be "other financial accounts" under the BSA, taxpayers may be forced to make educated guesses concerning whether particular records are producible or not. Consequently, as applied to government requests for "other financial accounts" under the BSA, Title 31 subpoenas arguably lack reasonable particularity and require a discretionary mental process sufficient to trigger Fifth Amendment protections for the taxpayer.

4. Foregone Conclusion Doctrine

A third exception to the act of production privilege is the foregone conclusion doctrine. Courts have found that, where the existence, possession or control, and authenticity of the compelled documents are a foregone conclusion, the Fifth Amendment privilege is not violated.[82] In such a case, the issue of compelled production becomes a "question … not of testimony but of surrender."[83] In these situations, the "tacit averments" of the taxpayer in producing the documents would not rise to the level of testimony within the protection of the Fifth Amendment because any information implicitly conceded in producing the documents is already within the Government's knowledge.[84]

In *W.L. Hubbell*, the Supreme Court set forth the standard for establishing the Government's knowledge of summonsed or subpoenaed records. It found that it must have *actual* knowledge of the existence and location of the compelled documents.[85] In so holding, it indicated that the Government cannot cure the lack of actual knowledge as to the existence and location of particular documents with broadly worded subpoenas and general arguments.[86] Such would make it "unquestionably necessary for [a taxpayer] to make extensive use of 'the contents of his own mind' in identifying … documents responsive to the requests in the subpoena."[87] In such a case, that taxpayer would effectively be providing a "catalog of existing documents" that was a "link in the chain" of his prosecution.[88]

More recently, in *S. Greenfield*, the Second Circuit clarified the necessary extent of the Government's actual knowledge.[89] In so doing, it noted that the Government must only establish knowledge with "reasonable particularity."[90] However, "it must know, and not merely infer, that the documents sought exist, that they were under the control of the defendant, and that they were authentic."[91] More importantly, the Court ruled it was insufficient for

the Government to show that the compelled documents once existed or were possessed by the taxpayer; rather the Government must show the documents existed and were possessed by the taxpayer "when the relevant summons [or subpoena] was issued."[92]

In addition to existence and control, the Government must establish that it could authenticate the desired records. In so doing, it must establish not only that the documents "are in fact what they purport to be," but also that the taxpayer will not be forced "to use his discretion in selecting … the responsive documents … thereby tacitly providing identifying information."[93] Normally, courts require the Government to "show only that it could [authenticate the documents] without the taxpayer's assistance, including without information gleaned from the documents."[94] However, when controversy exists concerning the source of particular documents, at least one court has indicated that the Government must go one step further by providing evidence of the identity and availability of the authenticating witness.[95]

In order for the Government to establish the applicability of the foregone conclusions doctrine with respect to crypto records, it must identify and acquire as much information as possible about the records they are seeking. It has numerous tools in its arsenal for doing so. In addition to John Doe summonses and FATCA information sharing, the Government may request or compel wallet information through third-party summonses, grand jury subpoenas, cooperation agreements, Tax Treaties, Mutual Legal Assistance Treaties ("MLATs"),[96] letters rogatory, and letters of request pursuant to the Hague Evidence Convention.

Thus far, Government efforts to acquire records of noncompliant crypto holders appear to be focused on the wallets of custodial exchanges.[97] To the extent taxpayers use domestic exchanges, it is likely to be able to acquire such custodial wallet records without the need for the foregone conclusion doctrine. However, it may be less successful in getting custodial wallet records from foreign exchanges. Often times, differences in laws, customs, and interpretations of international agreements result in the Government receiving less than perfect information in these situations. Nonetheless, armed with such imperfect information, the Government may still be able to use the foregone conclusion doctrine to compel complete foreign wallet records from the taxpayer.[98]

Just because the Government may be able to establish the applicability of the foregone conclusion doctrine with respect to particular custodial wallets does not mean that it will be able to do the same for other wallets.[99] To the contrary, it must separately prove the applicability of the foregone conclusion doctrine for each wallet it seeks.[100] To the extent the Government's ability to meet these standards is exceeded by what it is compelling in the summons or subpoena, courts have generally limited the scope of their compulsion orders to the records for which the Government can establish the applicability of the foregone conclusion doctrine.[101]

Where the Government is able to obtain custodial wallet records but seeks the records of other taxpayer wallets, it must independently develop leads from available information to identify the other wallets.[102] To this end, taxpayers can expect the Government to review known custodial wallet records for common wallet addresses sending and receiving crypto. For crypto users that change the address of their wallets each time they enter into a transaction, such an exercise is likely to prove unfruitful. However, for those that don't, it is possible that the Government could use those common wallet addresses to identify wallets associated with the custodial wallet. Additionally, using these discovered wallets, it could potentially run data analytics to identify common wallet addresses to those wallets. Through this type of investigative work, the Government could identify a network of wallets that are potentially controlled by the taxpayer. As a result, criminal tax attorneys representing non-compliant taxpayers should review any crypto wallet records the Government already has or is likely to acquire for common wallet addresses.

Even if the Government was able to identify other wallets that appear to be related to known taxpayer wallets, it would still need to establish that the taxpayer and not some third-party controlled those wallets.[103] To the extent the Government did not possess evidence that the taxpayer was a participant to a transaction entered into by one or more of these wallets, it will likely attempt to acquire and review bank records, emails, IP address information, and tax return information[104] for evidence that these wallets were opened, accessed, or paid for by the taxpayer. As a result, attorneys representing noncompliant crypto holders should interview their clients about the types of records the Government could acquire and use to find such evidence. Nonetheless, even if the Government were able to prove such a nexus, it would still need to establish that the taxpayer's control extended to the time the summons or subpoena was issued.[105]

As described earlier, the Government generally bears the formal and informal burden of proving a tax liability in criminal tax cases. In many crypto cases, this will necessitate proof of cost basis. For taxpayers that hold coins in and transfers them among multiple wallets, one wallet may be insufficient for the Government to establish such basis. To the extent it must acquire multiple wallets to do so, the

Government will need to establish the applicability of the foregone conclusion doctrine or another exception to the act of production doctrine with respect to each and every one. If it can't, the Government may have no choice but to decline to prosecute the taxpayer for the unreported crypto sales.

5. Search Warrant Issues

To the extent the Government can establish probable cause, it may choose to forgo the issuance of a summons or subpoena altogether in favor of applying for a search warrant for the desired crypto records. However, due to security concerns relating to private keys, many crypto users encrypt their wallets with passwords. In situations where the Government successfully seizes devices containing crypto wallets but cannot break the wallet encryption, it may decide to compel the encryption password from the taxpayer.

The Government typically compels encryption passwords for seized items by making an application for a court order pursuant to The All Writs Act.[106] In the few cases that have addressed this issue, courts have held that the act of providing compelled passwords to the Government for encrypted documents on seized devices may be sufficiently incriminating and testimonial to trigger the Fifth Amendment act of production privilege.[107] However, as with summonses and subpoenas for records, this privilege can be overcome if the Government can establish the applicability of the foregone conclusion with independent evidence.[108]

Few courts have addressed the foregone conclusion doctrine in the context of encryption passwords. The first series of cases addressing this issue used a framework that is virtually identical to that applied to Fifth Amendment assertions of privilege with respect to compelled documents.[109] Specifically, these cases analyze whether the Government could, with reasonable particularity, independently establish that the existence, authenticity of, and taxpayer's control over the files protected by the password are a foregone conclusion.[110] Nonetheless, recently, other courts have either indicated or held that the focus of the foregone conclusion doctrine in the context of compelled passwords should not be on the underlying files themselves.[111] Rather, since it is the password that is being compelled, the focus should be on whether the Government can independently establish that the target knows the password.[112]

In most unreported crypto tax cases, the two approaches will lead to the same conclusion and, thus, render arguments concerning the correct legal framework largely academic. However, this is not always the case. Given the sparse body of law in this area and the lack of agreement among courts, practitioners faced with these issues should carefully consider the flaws in each approach in formulating a position.

A foregone conclusion analysis that focuses only on the wallet itself is arguably misplaced because it ignores what the taxpayer is being compelled to produce—the encryption password. Control of a wallet and control of a password to that wallet do not necessarily go hand-in-hand. For example, a taxpayer and another person could share a wallet protected by an encryption password known only to the other person. While the taxpayer could control this wallet for periods of time upon the other entering the encryption password, that taxpayer would truly not be able to provide that password if compelled by the court to do so. In this scenario, the Government could potentially establish the taxpayer's control over the wallet itself *via* his or her transactional activity. If so, to the extent that a court focused its foregone conclusion doctrine analysis on the wallet itself rather than the password to that wallet, the taxpayer could find himself or herself in the absurd position of having to comply with an impossible court order to provide a password unknown to him or her or face jail time for contempt of court.

A foregone conclusion framework that focuses only on the password itself presents different but equally troubling issues. "The Fifth Amendment is inapplicable where the testimonial act does not create a related risk of self-incrimination."[113] There is no doubt that the production of a password implicitly admits that the taxpayer knows that password.[114] However, without context, such an admission is not incriminating.[115] As the Supreme Court has noted, questions about whether a taxpayer's tacit averments are testimonial and incriminating "do not lend themselves to categorical answers; their resolution may instead depend on the facts and circumstances of particular cases or classes thereof."[116] In unreported crypto encryption cases, context is important. By the time that the taxpayer attempts to invoke the Fifth Amendment concerning the act of producing an encryption password, the Government would have likely already seized the device containing the concerned wallet. If the contents of that wallet are incriminating, one could argue that the taxpayer implicitly admits a lot more than just knowledge of the password when he or she provides it. In these circumstances, knowledge of the password is likely to be characterized by the Government as an implicit admission of control over the encrypted wallet itself. Such an implicit admission seems to be sufficiently testimonial and incriminating to trigger Fifth Amendment protections. If so, it follows that the Government should also be required to establish that the

taxpayer's control over the wallet is a foregone conclusion in order to preclude him or her from invoking the act of production doctrine.

In light of the inherent flaws in each of these respective approaches, practitioners should consider taking the position that the Government be required to establish the applicability of the foregone conclusion doctrine under both approaches. Specifically, it should be required to establish, with reasonable particularity, independent knowledge that the taxpayer both knows the encryption password and controls the wallet protected by that encryption.

As the Government ramps up its unreported crypto tax enforcement campaign, taxpayers and their advisors may soon find themselves with the difficult decision of whether to comply with summonses, subpoenas, and court orders for incriminating crypto records or invoke the Fifth Amendment act of production privilege. Although assertions of this privilege have been largely unsuccessful in recent years in the context of offshore banking cases, the manner in which crypto is held and used by taxpayers gives rise to more promising arguments and strategy for those seeking to legally shield themselves from Government compulsion. With the assistance of an experienced criminal tax attorney, taxpayers may be able to repel Government efforts to obtain incriminating wallet records and, in turn, cause prosecutors to decline to prosecute them for unreported crypto.

ENDNOTES

* Kevin F. Sweeney is currently a Senior Counsel in the Philadelphia Office of Chamberlain Hrdlicka where he focuses on IRS audits, civil and criminal tax litigation, and corporate investigations. Kevin may be reached at (610) 772-2327 or by email at *ksweeney@chamberlainlaw.com*.

1 *IRS Acknowledges that Cryptocurrency Is a Threat* (May 10, 2018) *www.winston.com/en/thought-leadership/irs-acknowledges-that-cryptocurrency-is-a-threat.html*.

2 *IRS Announces the Identification and Selection of Five Large Business and International Compliance Campaigns* (July 2, 2018), *www.irs.gov/businesses/irs-announces-the-identification-and-selection-of-five-large-business-and-international-compliance-campaigns*.

3 *Doe*, 465 US 605, 611–612 & n. 10 (1984).

4 U.S. CONST. amend. V.

5 *S. Fisher*, SCt, 76-1 USTC ¶9353, 425 US 391, 408, 96 SCt 1569 (1976).

6 *J. Doe*, SCt, 88-2 USTC ¶9545, 487 US 201, 210, 108 SCt 2341 (1988).

7 *S. Fisher*, 425 US 408.

8 *S. Fisher*, 425 US 410.

9 *Id.*

10 *E. Chabot*, CA-3, 2015-2 USTC ¶50,388, 793 F3d 338, 342.

11 See the Required Records Doctrine for further explanation of the different types of crypto wallets.

12 When possession of the private key is transferred from the sender to the recipient, a new number and letter combination will be generated and provided to the buyer.

13 Some crypto exchanges offer special wallets designed to facilitate currency conversions and the transfer of U.S. dollars to and from bank accounts.

14 In most cases, personal wallets encrypt a user's private keys as an additional security measure.

15 The Required Records Doctrine section contains a more detailed description of what is meant by a custodial exchange.

16 Wolfie Zhao, *Coinbase Tells 13,000 Users It's Sending Their Data to the IRS* (Feb 26, 2018), *www.coindesk.com/coinbase-tells-13000-users-its-sending-their-data-to-the-irs/*.

17 Ana Alexandre, *Bitfinex Requires Customer Tax Info Which it May Exchange with Gov't, Tax Authorities* (May 18, 2018), *https://cointelegraph.com/news/bitfinex-requires-customer-tax-info-which-it-may-exchange-with-govt-tax-authorities*.

18 These exchanges track this fungible value based on coin units. This may give users the appearance that they are holding, purchasing, and selling particular coins when, in fact, they are not.

19 Even when the charged offenses do not necessarily require proof of a tax liability, the Government would nonetheless likely not bring a case in which it could not establish one because it risks jury nullification and is unlikely to result in a sentence sufficient to produce a general deterrent effect.

20 *See* Notice 2014-21; Neither the Service nor the courts have further classified crypto as a particular type of property for tax purposes. Some practitioners have argued that, in Notice 2014-21, the Service classifies it as intangible property. More recently, a federal district court judge found that crypto is a commodity for the purposes of U.S. Commodity Futures Trading Commission ("CFTC") jurisdiction. *See CFTC v. McDonnell*, No. 18-cv-0361, Dkt. 29 (E.D.N.Y. Filed Jan. 18, 2018). It reasoned that "virtual currencies are 'goods' exchanged in a market for a uniform quality and value…" Moreover, in a recent interview with CNBC, the Chairman of the U.S. Securities and Exchange Commission ("SEC") stated, with respect to crypto tokens that "a digital asset, where I give you my money and you go off and make a venture, and in return for giving you my money I say 'you can get a return'[;] that is a security and we can regulate that." *See www.cnbc.com/2018/06/06/sec-chairman-clayton-says-agency-wont-change-definition-of-a-security.html*. However, crypto tokens are vastly different than cryptocurrency, which the SEC has not stated is a security.

21 *Id*.

22 *See* 26 USC §1221.

23 Generally, the Government satisfies its burden of proof when it shows that the taxpayer has received more income than was reported. *See A. Bender*, CA-7, 55-1 USTC ¶9142, 218 F2d 869, 871. It typically need not prove an exact amount of tax deficiency. *See W.R. Johnson*, SCt, 43-1 USTC ¶9470, 319 US 503, 517–518, 63 SCt 1233 (1943).

24 *See S. Dworskin*, CA-5, 81-1 USTC ¶9416, 644 F2d 418, 434 n. 4 (finding that the Government had burden of proving a prima facie tax due and owing); *See also J.P. Schroeder*, CA-7, 2008-2 USTC ¶50,477, 536 F3d 746 (finding the Government has the burden of proving tax loss at sentencing); U.S. Dep't of Justice, Criminal Tax Manual §12.10[5] (noting that the lack of a tax liability may be probative of the materiality element of Code Sec. 7602(1).

25 *See* Reg. §1.61-6(a); Section 1011 of the Internal Revenue Code characterizes the term "cost or other basis" as adjusted basis. Code Sec. 1012, in turn, specifies that the adjusted basis of property sold or exchanged shall be the cost of the property unless otherwise specified. This method of determining basis is more commonly known as specific identification. No other rules concerning the basis of crypto held as a capital asset are specified in the Internal Revenue Code, Treasury Regulations, or Service publications.

26 *See* Reg. §1012-1(a). Some practitioners have posited that, in light of the fungible nature of crypto, the Service may permit cost basis to be computed using the FIFO method consistent with analogous regulatory exceptions for fungible corporate stock. See Reg. §1012-1(c). While the Service may very well permit this treatment in civil cases, there is no statutory or regulatory basis for computing cost basis in this manner.

Consequently, in a criminal case, practitioners should consider holding the Government to the more difficult burden of applying the specific identification method.

[27] Since coins sales only constitute income to the extent they exceed cost basis, it follows that the burden is on the Government to prove cost basis. *See L. Small*, CA-1, 58-2 USTC ¶9553, 255 F2d 604, 607 (noting that, with respect to the sale of real property, the initial burden was on the Government to establish both the sales price of a home and the original cost but that, once met, the burden shifted to the defendant to prove any additional items that could be applied against the sales price).

[28] *See Helvering v. Rankin*, SCt, 35-1 USTC ¶9343, 295 US 123, 125, 55 SCt 732 (1935) (acknowledging, with respect to margin trading of another type of fungible property—corporate stock, that "the identification of sales and purchases is frequently impossible").

[29] The Government is also likely to face situations where both issues are present. For instance, when a taxpayer transfers a particular coin into a custodial wallet with existing fungible crypto and then sell a portion of the total amount of the crypto in that wallet on the exchange, the Government will need to decide how to compute the cost basis of the fungible crypto sold, how to determine the purchase price of the coin transferred into the wallet, and what the effect of information learned about the purchase price of that particular coin or lack thereof will have on its cost basis computations. None of these issues have ever been addressed by the Service or decided by a court.

[30] With respect to coins transferred from a taxpayer's personal wallet to a wallet provided by a custodial exchange, it is possible that the Service could take the position that such transfer constitutes a taxable exchange. This is because the taxpayer is essentially exchanging a particular coin akin to a gold bar for fungible value akin to a share of a gold fund. However, such a position would not be practically intuitive for taxpayers and would arguably run counter to the Service's treatment of another type of fungible property—corporate stock. *See generally* Reg. §1012-1(c). For example, when a taxpayer transfers a physical stock certificate representing a share of a corporation to a brokerage that, in turn, holds the share on his or her behalf in "street name," the transfer is typically not considered a taxable event. This is so even though it technically results in a transfer of ownership from the taxpayer to the brokerage which, in turn, documents the taxpayer's holdings in its internal records.

[31] The Government would not be able to simply trace the blockchain because, while it would establish the dates on which the coin was transferred, it would not identify the participants to those transfers.

[32] *See Novotny*, 184 FSupp2d 1071, 1082 (D. Col. 2001).

[33] To the extent a non-attorney practitioner inquiries about the existence of a taxpayer's records and finds records indicating he or she had significant unreported crypto, that representative risks becoming a government witness and may actually be used by the government to establish the applicability of the foregone conclusion doctrine. See the Section on the Foregone Conclusion Doctrine for more details. One way to mitigate this risk would be for the taxpayer to retain a criminal tax counsel who, in turn, hired the accountant under *Kovel* arrangement for the purpose of advising on IDR or summons responses and/or potential Fifth Amendment issues.

[34] *See Hale v. Henkel*, 201 US 43, 69–70, 74 (1906).

[35] *See Wilson*, 221 US 361 (1911); *I. Bellis*, SCt, 88-2 USTC ¶9546, 417 US 85, 108 SCt 2284 (1974); *Doe*, 465 US 605 (1984); *R. Braswell*, SCt, 88-2 USTC ¶9546, 487 US 99, 108 SCt 2284 (1988).

[36] *Id.*

[37] *Id.; See also e.g., Roe*, 421 F. App'x 881, 884–885 (10th Cir. 2011); *Lu*, 248 F. App'x 806, 807–808 (9th Cir. 2007).

[38] Miners validate crypto transactions in the blockchain via a distributed consensus system as part of a third-party network.

[39] *See Wilson*, 221 US 380.

[40] *See E.H. Peter*, CA-6, 73-1 USTC ¶9461, 479 F2d 147, 149 ("Appellant could not clothe the records of his two corporations with immunity by mingling them with his personal records.").

[41] *In re Sealed Case (Government Records),* 950 F2d 736, 740–741 (D.C. Cir. 1991).

[42] *Id.*; *See also In re Grand Jury Subpoena Duces Tecum Dated April 23, 1981*, 522 FSupp 977, 979 (S.D.N.Y. 1981). While these cases have held that it is technically possible to sever out personal records from corporate records, neither case set forth procedures for doing so. Given that an admission of the existence and taxpayer's possession and control over the documents would likely result in the Government invoking the foregone conclusion doctrine, the taxpayer would have to be extremely careful in how he or she raises the issue. If at all possible, taxpayers in this situation should designate a corporate custodian to raise the issue with the court on behalf of the legal entity business.

[43] *Shapiro*, 335 US 1, 33 (1948).

[44] *J. Marchetti*, SCt, 68-1 USTC ¶15,800, 390 US 39, 88 SCt 697 (1968).

[45] *A.M. Grosso*, SCt, 68-1 USTC ¶15,801, 390 US 62, 88 SCt 709 (1968).

[46] *In re Grand Jury Subpoena Duces Tecum Served Upon Underhill*, 781 F2d 64, 67 (6th Cir.) (quoting *A.M. Grosso*, 390 US 67–68).

[47] *H.V. Porter*, CA-7, 83-2 USTC ¶9457, 711 F2d 1397; *See also* Code Sec.6001 (providing, in part, that "[e]very person liable for any tax imposed by this title, or for the collection thereof, shall keep such records, render such statements, make such returns, and comply with such rules and regulations as the Secretary may from time to time prescribe").

[48] *Id.*; *See also Smith v. Richert*, 35 F3d 300 (7th Cir. 1994) (finding that documents sought by state revenue agent subpoena, asking taxpayer to produce "books, accounts ... receipts, invoices, cancelled checks and any other records" necessary to determine income tax liability were not "required records" for purposes of required records doctrine, and that taxpayer was not member of regulated industry).

[49] *See J. Cianciulli,* 2002-2 USTC ¶50,555 (S.D.N.Y. 2002); *Whitehouse*, 106 A.F.T.R.2d 2010-7124, 2010 WL 4876295 (D. Conn. 2010); *But see Smith v. Richert*, 35 F3d 300 (7th Cir. 1994) (finding that documents sought by state revenue agent subpoena, asking taxpayer to produce "Forms W-2, Forms 1099" necessary to determine income tax liability were not "required records" for purposes of required records doctrine).

[50] *In re Grand Jury Investigation M.H.*, 648 F3d 1067.

[51] *Id.*

[52] *In re M.H.*, 648 F3d 1079.

[53] *In re M.H.*, 648 F3d 1074.

[54] *In re M.H.*, 648 F3d 1076.

[55] *In re M.H.*, 648 F3d 1077–1090.

[56] There is little guidance concerning how to determine what particular foreign country an account is located in. However, in *Hom*, the Northern District of California and Ninth Circuit collectively found that it is based on where the company holding the account is located and licensed and, in turn, where the account was created and maintained. *Hom*, No. 14-16214 (9th Cir. 2016); *Hom*, No. C 13-03721 WHA, 2014 WL 2527177 (N.D. Cal. June 4, 2014).

[57] 31 CFR §1010.350(a).

[58] 31 CFR §1010.420 (providing that taxpayers must maintain foreign financial records that contain (1) "the name in which each such account is maintained"; (2) "the number or other designation of such account"; (3) "the name and address of the foreign bank or other person with whom such account is maintained"; (4) "the type of such account"; and (5) "the maximum value of each such account during the reporting period").

[59] 31 CFR §1010.350(c)(3).

[60] 31 USC §5312(a)(1).

[61] Department of the Treasury Financial Crimes Enforcement Network, *FIN-2013-G001 Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies* (March 18, 2013) *available at www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf*.

[62] IRM 4.26.16.3.2.3.

[63] *Id.*

[64] *Id.*

[65] *See generally* Peter Van Valkenburgh, *The Bank Secrecy Act, Cryptocurrencies, and New Tokens: What Is Known and What Remains Ambiguous*, Coin Center Report (May 2017) available at *https://coincenter.org/entries/aml-kyc-tokens*.

[66] These wallets are typically web-based.

[67] Some custodial exchanges like LocalBitcoins use a decentralized platform that resembles a peer-to-peer exchange in some ways. However, the private keys of coins bought and sold using its wallets are still controlled by the exchange itself.

[68] FinCEN, *FIN-2014-R002 Application of FinCEN's Regulations to Virtual Currency Software Development and Certain Investment Activity* (Jan. 30, 2014) *www.fincen.gov/sites/default/files/shared/FIN-2014-R002.pdf* (emphasis added) (but also noting "should the Company begin to engage as a business in the exchange of virtual currency against currency of legal tender (or even against other convertible virtual currency), the Company would become a money transmitter under FinCEN's regulations.").

[69] Department of the Treasury Financial Crimes Enforcement Network, *FIN-2013-G001 Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies* (Mar. 18, 2013) available at *www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf.*

[70] When a taxpayer transfers particular coins into a custodial wallet for fungible value, he or she also transfers the private keys of those coins and grants the exchange the unfettered ability to dispose of them.

[71] Conversely, the BSA does not require the maintenance of records beyond five years and, thus, compelled records of transaction occurring beyond this time frame should not fall within the required records doctrine. The Second Circuit indicated as much in *S. Greenfield* when it noted:

> The Government can require an individual to produce documents related to foreign bank accounts maintained pursuant to the [BSA] and its implementing regulations, see 31 CFR §1010.420, without violating an individual's right against self-incrimination under the Fifth Amendment … The Summons in this case, however, seeks documents that fall outside the five-year period under the BSA during which an individual is required to maintain documents by law. *S. Greenfield*, CA-2, 2016-2 USTC ¶50,367, 831 F3d 106, 115 n. 6 (2d Cir. 2016).

[72] *In re Grand Jury Subpoena Dated Sept. 12, 2011*, 691 F3d 908–909; *In re Grand Jury Proceedings*, No. 4-10, 707 F3d 1274; *Ali,* 2014 WL 5790996 (D. Mar. Nov. 5, 2014); *Chen*. 952 FSupp2d 321, 332 (D. Mass. 2013).

[73] *See also Smith v. Richert*, 35 F3d 303 (stating the "hypothetical case in which every individual is required to maintain a record of everything he does that interests the government is remote from the case of the individual who enters upon a regulated activity knowing that the maintenance of extensive records available for inspection by the regulatory agency is one of the conditions of engaging in the activity").

[74] In determining whether the required records doctrine applies, courts have generally declined to consider a taxpayer's ignorance of the statute at issue as well as arguments that the statute does not apply to the particular taxpayer. *See In re Grand Jury Subpoena Dated Feb. 2, 2012*, 741 F3d 339, 352 (2d Cir. 2013) (finding, based on the defendant's factual argument that foreign bank account beneficiaries are frequently unaware of their settled requirements under the BSA, that ignorance of the law is no defense to the required records doctrine); *See also In re M.H.,* 648 F3d 1079 (finding that the court need not make a factual determination about whether the BSA applied to the particular defendant "as a U.S. taxpayer who has previously filed FBARs with the Department of the Treasury"). Consequently, taxpayers making this argument should emphasize that it is not based on their specific knowledge of BSA requirements (or lack thereof) or the applicability of these requirements to their particular factual situation but rather on the basis that the applicability of BSA requirements to foreign crypto wallets is categorically unsettled as a matter of law. Obviously, if the BSA was found to not apply to foreign crypto wallets, the government would not be able to use it as a basis for compelling foreign crypto wallet records. It would seem that it should, likewise, not be able to use it for this purpose while the issue remains unsettled because, during this time, taxpayers would have no way of knowing with certainty whether or not the BSA requirements apply to foreign crypto activity and, thus, no way of knowing whether the maintenance of such records are a condition of entering into this activity.

[75] The application of the required records doctrine to unsettled questions about the BSA's reach could produce absurd results. There was similar uncertainty concerning whether an investment in a hedge fund was subject to FBAR reporting requirements prior to 2011. During this time period, several senior IRS personnel had indicated that such investments may be subject to these requirements. *See*, *e.g.*, Paul, Hastings, Janofsky & Walker, LLP, "'FBAR' Filing Requirement May Apply to Interests in Foreign Pooled Investment Funds; IRS Has Issued New Guidance on June 30 Filing Deadline," *StayCurrent, A Client Alert from Paul Hastings*, p. 2 (June 2009). However, in 2011, the BSA regulations were updated to reflect that such investments were, in fact, not subject to FBAR requirements so long as the investments were not offered to the public. Preamble to final RIN 1506-AB08, 76 FR 10234, 10239 (2/24/11); 31 CFR 1010.350(c)(3)(iv)(A). Hypothetically speaking, if the DOJ was able to apply the required records doctrine to unreported hedge fund investment records prior to 2011 despite the uncertainty, concerned taxpayers would have been precluded from asserting their Fifth Amendment privileges pursuant to the required records doctrine even though those compelled records would be determined in subsequent years to be, in fact, not required under the BSA at all. Such a result would defy all rationale for the required records doctrine.

[76] American Institute of Certified Public Accountants, *Updated Comments on Notice 2014-21: Virtual Currency Guidance* (May 30, 2018) (noting that taxpayers still have no guidance on whether crypto is reportable on an FBAR); American Bar Association Section of Taxation, *Comments Regarding the OVDP and Streamlined Procedures* (May 2, 2018) (noting that it is unclear whether foreign crypto wallets are subject to a FBAR requirement).

[77] American Institute of Certified Public Accountants, *Comments on Notice 2014-21: Virtual Currency Guidance* (June 10, 2016) (noting that, based on its intangible and virtual nature, it does not appear that crypto has any location, which complicates its foreign compliance reporting). Digital crypto wallets are really just software, which hold computer files in the form of cryptographic keys. Such keys are not actually assets themselves but rather prove that assets, crypto coins, exist and are owned by the wallet holder. Despite the fact that proof of the existence and ownership of crypto coins may sit on a wallet stored on the server of a non-U.S. company, the coins themselves arguably do not exist in any one location because they have no physical form.

[78] Rod Lundquist, a senior program analyst for the Small Business/Self-Employed Division, stated in a webcast that, for FBAR purposes, Bitcoin is not reportable "…not at this time." Lundquist also stated that "FinCEN has said that virtually currency is not going to be reportable on the FBAR, at least for this filing season," broadcasted June 4, 2014, see archived webcast: *www.irsvideos.gov/ElectronicFBAR/; https://www.wsj.com/articles/do-you-own-bitcoin-the-irs-is-coming-for-you-1521192601* (stating "according to a Treasury unit, investors aren't currently required to report cryptocurrency holdings on FinCen Form 114, known as the Fbar, which is often required for foreign accounts greater than $10,000.); *www.lawfirmwolf.com/virtual-currency-and-fbar-reporting* (stating that "Right now, we have not put out any guidance on reportability of bitcoin or any other virtual currency as part of FBAR. That being said, we do not expect it to be reported," Jeremy Kuester, deputy associate director for policy at FinCEN, said at the American Institute of CPAs' National Tax Conference on November 7th, in Washington. "As the regulations are currently written, a virtual currency wallet would not fall under our definition of an account." Kuester added that FinCEN may still consider putting out official guidance since it is still continuing to monitor the evolving situation.).

[79] *D.R. Garber*, CA-5, 79-2 USTC ¶9709, 607 F2d 92, 100.

[80] *Alewelt*, 532 F2d 1165, 1168 (7th Cir.1976) (citations omitted) (emphasis added).

[81] *In re Grand Jury Subpoena Duces Tecum Served on Allied Auto Sales, Inc.*, 606 FSupp 7, 13, n. 5 (D. R.I. 1983).

[82] *Greenfield*, 831 F3d 115 (citing *S. Fisher,* 425 US 411) (citations omitted).

[83] *S. Fisher*, 425 US 411 (quoting *In re Harris*, 221 US 274, 279 (1911)).

[84] *See P.D. Rue*, CA-8, 87-1 USTC ¶9346, 819 F2d 1488 (8th Cir. 1987).

[85] *W.L. Hubbell*, SCt, 2000-1 USTC ¶50,499, 530 US 27, 30–31, 120 SCt 2037 (2000).

[86] *W.L. Hubbell,* 530 US 45.

[87] *W.L. Hubbell,* 530 US 42.

[88] *Id.*

[89] *S. Greenfield*, CA-2, 2016-2 USTC ¶50,367, 831 F3d 106.

[90] *S. Greenfield*, 831 F3d 116.

[91] *Id.*; *See also B.K. Bright,* CA-9, 2010-1 USTC ¶50,249, 596 F3d 683, 692 (noting that the Government bears the burden of proving that it had the requisite knowledge); *D.L. Norwood*, CA-8, 2005-2 USTC ¶50,542, 420 F3d 888, 895–896 (applying the foregone conclusion doctrine when the Government could demonstrate the existence of account documents even though it did not specify the particular responsive documents).

[92] *S. Greenfield*, 831 F3d 124.

[93] *Sideman & Bancroft LLP*, CA-9, 2013-1 USTC ¶50,135, 704 F3d 1197, 1203 (internal quotation marks omitted).

[94] *B.K. Bright,* 596 F3d 693.

[95] *S. Greenfield*, CA-2, 2016-2 USTC ¶50,367, 831 F3d 106.

[96] To the extent that a practitioner learns that a crypto investigation began based on wallet records compelled by a foreign sovereign, he or she should inquire into the circumstances. Several countries including the U.K. and Australia have key disclosure laws that require individuals, in certain circumstances, to surrender to the foreign sovereign the password to encrypted files including crypto wallets. These key disclosure laws are criminally punishable. See John Matonis, *Key Disclosure Laws Can Be Used to Confiscate Bitcoin Assets* (Sept. 12, 2012), *www.forbes.com/sites/jonmatonis/2012/09/12/key-disclosure-laws-can-be-used-to-confiscate-bitcoin-assets/#775ebf22ef54*. An encryption password that is secured by a foreign sovereign through the use of a law like this is likely to be determined by a U.S. court to be involuntarily compelled and, thus, acquired in violation of the Fifth Amendment. To be admissible in a U.S. court, inculpatory statements obtained overseas by foreign officials must have been made voluntarily. *Allen*, 864 F3d 63 (2d Cir. 2017). Importantly, as the Second Circuit recently confirmed in this context, the Government's derivative use of such evidence has also been found to violate a defendant's Fifth Amendment rights. *Id.* Consequently, any evidence developed by U.S. authorities based on such evidence would likely be excluded as fruit of the poisonous tree.

[97] It seems that this is, in part, based on the difficulties in identifying non-custodial wallets and, in part, based on the reality most non-custodial wallet providers likely keep little to no records concerning their users.

[98] *See generally B.K. Bright,* CA-9, 2010-1 USTC ¶50,249, 596 F3d 683; *D.L. Norwood*, CA-8, 2005-2 USTC ¶50,542, 420 F3d 888.

[99] *Id.*

[100] *Id.*

[101] *Id.*

[102] *Id.*

[103] With respect to non-custodial wallets, it remains to be seen what the Government must prove in order to establish the authenticity prong. However, it is possible that the Government may have an easier time authenticating crypto then it did with offshore bank accounts. In recent cases concerning a different type of cryptographic technology—encryption passwords—courts have tended to overlook, brush past, or presume this prong for reasons not thoroughly explained. See *In re Search of a Residence in Aptos, Calif. 95003*, No. 17-mj-70656-JSC, 2018 WL 1400401 (N.D. Cal. Mar. 20, 2018). A recent Florida state court opinion may shed on light on the reasons why. In that case, the court noted that "if the [foregone conclusion doctrine is] to continue to be applied to passcodes, decryption keys, and the like, we must recognize that the technology is self-authenticating—no other means of authentication may exist." *State v. Stahl*, 206 So.3d 124, 136 (Fla. Dist. Ct. App. 2016). That Court ultimately concluded that, "if the phone or computer is accessible once the passcode or key has been entered, the passcode or key is authentic." *Id.* Applying this logic, it is possible that federal courts will similarly find that crypto is self-authenticating in that the private keys in the taxpayer's wallets can be validated by matching them to the respective public keys in the blockchain.

[104] A review of the taxpayer's returns will likely, alone, be insufficient to establish the applicability of the foregone conclusion doctrine. In *M. Fox*, the Second Circuit found that "the mere fact that a tax return reveals on its face that a taxpayer had 'at least one bank account' or 'brokerage account' does not give the IRS any information about whether the taxpayer has records of other bank accounts showing income that was never reported in his return." CA-2, 83-2 USTC ¶9660, 721 F2d 32, 37–38 (internal citations omitted). In fact, with respect to crypto, it is unlikely that the return will provide evidence that the taxpayer uses any particular exchange. Instead, it will generally only reflect the type of crypto coin that was sold. Nonetheless, to the extent that a return become due or the decision to filed amended returns is made during an audit or criminal investigation, taxpayers should consult a criminal tax attorney concerning whether or not to take the Fifth Amendment with respect to crypto related items on those returns. *See generally R. Neff*, CA-9, 80-1 USTC ¶9397, 615 F2d 1235, 1239; *M.S. Sullivan*, SCt, 1 USTC ¶236, 274 US 259, 263–264, 47 SCt 607 (1927); *R.D. Garner*, CA-9, 75-1 USTC ¶16,185, 501 F2d 228, 252, n. 18, *aff'd*, 76-1 USTC ¶16,218, 424 US 648, 96 SCt 1178 (1976).

[105] In most cases, the court is likely to allow the Government to draw an inference of continued existence and control but, where the nature of the documents and time lapses render the Government's evidence stale, this may not be enough. *S. Greenfield*, 831 F3d 125.

[106] *Apple Macpro Computer*, 851 F3d 238, 245 (3d. Cir. 2017); The All Writs Act is codified at 28 USC §1651, which authorizes the U.S. federal courts to "issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law"; Since crypto is based on encryption technology, it is conceivable that, in an asset forfeiture context, the Government could attempt to gain possession of one's crypto by simply making an application pursuant to The All Writs Act for the private key. However, this scenario is beyond the scope of this article.

[107] *Apple Macpro Computer*, 851 F3d 247; *In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011*, 670 F3d 1335, 1337 (11th Cir. 2012).

[108] *In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011*, 670 F3d 1346; *In re Search of a Residence in Aptos, Calif. 95003,* No. 17-mj-70656-JSC, 2018 WL 1400401.

[109] *In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011*, 670 F3d 1335.

[110] *Id.* In most of these cases, the existence of the encrypted files is not an issue because the Government already possesses the seized device that houses them.

[111] *In re Search of a Residence in Aptos, Calif. 95003,* No. 17-mj-70656-JSC, 2018 WL 1400401; *See Apple MacPro Computer*, 851 F3d 248, n. 7 ("a very sound argument can be made that the foregone conclusion doctrine properly focuses on whether the Government already knows the testimony … implicit in the act of production. In this case, the fact known to the Government that is implicit in the act of providing the password for the devices is "I, John Doe, know the password for these devices").

[112] *Id.*

[113] *In re Grand Jury Subpoena Dated Feb. 2, 2012*, 741 F3d 352.

[114] *In re Search of a Residence in Aptos, Calif. 95003*, No. 17-mj-70656-JSC, 2018 WL 1400401.

[115] For example, a disinterested third-party could know the password only because, before the electronic device was seized by the Government, he or she witnessed a post-it note stuck to the electronic device containing the password for the encrypted wallet.

[116] *S. Fisher*, 425 US 410.