Bloomberg BNA

White Collar Crime Report™

TAX EVASION

Evaders May Turn to Virtual Currency as Traditional Offshore Bank Secrecy Falters

BY PETER HARDY AND MEHREEN ZAMAN

Virtual currency has been in the media spotlight due to a cocktail of trends: entrepreneurial interest, cautionary tales of serious investor risk, technological wonder and increasing regulatory scrutiny, including some criminal charges alleging that virtual currency systems served as money-laundering conduits for drug dealing and other criminality.

Peter Hardy is a principal with Post & Schell PC in Philadelphia. Hardy previously served as an assistant U.S. attorney in Philadelphia and as a trial attorney in the Criminal Enforcement Section of the Justice Department's Tax Division in Washington. He is the author of ''Criminal Tax, Money Laundering, and Bank Secrecy Act Litigation,'' a legal treatise published by Bloomberg BNA. He can be reached at phardy@postschell.com.

Mehreen Zaman is an associate in the firm's Philadelphia office and is part of the firm's internal investigations and white collar defense practice. She can be reached at mzaman@postschell.com.

Both Hardy and Zaman have significant experience in representing corporations and individuals in matters involving allegations of financial fraud, including criminal tax, securities, money laundering and health-care fraud violations.

Very generally, virtual currency represents a digital unit of exchange that is not backed by a government. The most well-known example is bitcoin. Although there have been setbacks, its use and acceptance has been growing globally. The Internal Revenue Service now has turned its attention to virtual currency, recognizing that it may be the future of finance and that it certainly provides a current vehicle for potential tax evasion. Indeed, virtual currency may be poised to undermine the most remarkable advances in U.S. tax enforcement in recent history.

Since February 2009, when Swiss banking giant UBS AG agreed to disclose the names of certain U.S. customers as part of a deferred prosecution agreement with the Department of Justice[1] involving charges of tax fraud based on undisclosed accounts held by U.S. taxpayers, centuries of offshore bank secrecy practices have continued to erode. Offshore banking has been a focus of vigorous tax enforcement, both criminal and civil, by U.S. officials ever since.

Virtual currency currently has many of the (formerly) perceived advantages that traditional offshore bank accounts offered to would-be tax evaders: relative anonymity and difficulty in tracing.[2] Some U.S. taxpayers who find that their previously undisclosed money is no longer welcome at traditional foreign banks, either because of disclosure deals struck by those banks and their governments with the U.S. or because of upcoming reporting requirements for foreign banks,[3] may turn to virtual currency to try to shelter their assets.

---

[1] 04 WCR 134 (2/27/09).

[2] See generally Omri Marian, *Are Cryptocurrencies 'Super' Tax Havens?*, 112 Mich. L. Review First Impressions 38 (October 2013).

[3] The foreign reporting and withholding provisions of the Foreign Account Tax Compliance Act (FATCA), see 26 U.S.C. §§ 1471–74; § 6038D, oblige foreign banks and other foreign financial institutions (FFIs), as defined, to enter into an agreement with the IRS in which the FFI agrees to identify its U.S.

Traditional Weapons. Given these parallels, the IRS may invoke some of the weapons it has used effectively against traditional offshore bank accounts, including the report of foreign bank and financial accounts (FBAR) form pertaining to the disclosure of offshore accounts. However, as we discuss, any potential FBAR reporting requirements may turn on the particular technology used by a holder of virtual currency, making both enforcement by the government and compliance by individuals particularly difficult.

The future of virtual currency is an open question. It may be a fascinating but untenable experiment that will collapse under the combined weight of predatory hackers who will rob it of the security necessary for mass appeal and regulators who will seek to deprive it of one of its most defining features, that of relative anonymity. Alternatively, it may become as ubiquitous as the Internet and e-mail are now but in a form that mirrors the high state of regulation of traditional finance. Until these questions resolve—and given the clear attraction of virtual currency to people who prize both technological sophistication and a desire for anonymity—the broad and effective real-world enforcement of a virtual tax reporting system will be challenging.

The IRS Enters the Virtual Fray

The IRS is attempting to keep up with this swiftly evolving technology. As the use of virtual currency continues to spread, both domestically and particularly abroad, one conceivably could survive—or at least pursue an enhanced lifestyle—largely on unreported virtual currency. Although the IRS has made important strides in describing a basic regulatory framework for virtual currency, the real-world enforceability of that framework is currently very unclear.

In May 2013, the Government Accountability Office issued a report[4] to the Senate Committee on Finance, recommending that the IRS provide guidance on the tax implications of virtual currency, which—regardless of its precise categorization—can represent taxable income. In addition to acknowledging that virtual currency may serve as a vehicle for tax evasion given its degree of anonymity and difficulty in tracing, the GAO report recommended that the IRS issue guidance regarding third-party reporting requirements for virtual currency transactions. As tax enforcement officials know, the best way to maximize general compliance with tax requirements is through third-party reporting. A classic example: W-2 wage earners tend to report income with much greater accuracy than the self-employed.

The IRS recently responded to this GAO report and other pressures by issuing guidance in March on how existing general tax principles apply to transactions using virtual currency.[5] According to the guidance, virtual currency does not represent a ''currency'' for tax purpose; rather, it represents, and is taxable as, ''property'' according to the fair market value of any gains or losses, converted into U.S. dollars. As for third-party reporting, the guidance provides that virtual currency paid by an employer for services represents wages subject to employment taxes and income tax withholding. Moreover, virtual currency payments are subject to information reporting and backup withholding, such as Form 1099 reporting to the IRS and the payee, just like any other payments made with property. If a payer of virtual currency cannot obtain the required identification information from the payee to issue a Form 1099 (such as the payee's name, address and tax identification number), then taxes must be withheld. Presumably, compliance with this reporting system will be uneven at best, given the fact that many use virtual currency precisely because it is held out as a more anonymous vehicle to do business.

Thus, it still will be quite difficult for the government to catch many virtual tax evaders, particularly given the classic dilemma of limited tax enforcement resources. Although the use of virtual currency requires a shared public ledger of all transactions, thereby preventing the system from being truly anonymous, transactions are linked to digital addresses that, standing alone, do not reveal the user's actual identity. Although it is possible to trace virtual transactions by following this chain, such tracing would be very resource-intensive if tax investigators want to get the full picture of an individual's income rather than simply following the trail of a single transaction. Criminal tax investigations are demanding, and attempting to reconstruct a person's entire virtual financial history over several years will be significantly complex, if not impossible, particularly because one individual can use many different addresses for virtual transactions.

Virtual Currency and the Bank Secrecy Act

Prior to the IRS guidance, the leader in regulating virtual currency has not been the IRS. Rather, it has been another branch of the Department of Treasury, the Financial Crimes Enforcement Network (FinCEN), which is the regulator for the Bank Secrecy Act. In March 2013, FinCEN issued interpretive guidance[6] concluding that under the BSA, an ''administrator'' or ''exchanger'' of virtual currency is a ''money transmitter,''[7] which in turn qualifies as a ''money service business,''[8] or MSB, which in turn qualifies as a ''financial institution''[9] under the BSA.

The FinCEN guidance defines an ''administrator'' as someone who is engaged in the business of putting virtual currency into circulation and has the authority to withdraw such currency from circulation. Further, it defines an ''exchanger'' as someone engaged in the business of exchanging virtual currency for real currency or other virtual currency. However, FinCEN also concluded that a mere ''user'' of virtual currency, defined as a person who obtains virtual currency to purchase

account holders, obtain information from these account holders, report that information every year to the IRS and perform related due diligence.

[4] GAO-13-516, *Virtual Economies and Currencies: Additional IRS Guidance Could Reduce Tax Compliance Risks* (May 15, 2013), available at http://www.gao.gov/products/gao-13-516.

[5] IRS notice 2014-1 (March 25, 2014), available at http://www.irs.gov/uac/Newsroom/IRS-Virtual-Currency-Guidance.

[6] See FIN-2013-G001, *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies* (March 18, 2013), available at http://fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html.

[7] 31 C.F.R. § 1022.100(ff)(5)(i)(A).

[8] 31 C.F.R. § 1010.100(ff).

[9] 31 C.F.R. § 1010.100(t)(3).

  WCR ISSN 1559-3185

goods or services, is not a money transmitter.[10] Nonetheless, this FinCEN guidance still has enforcement implications for individuals possessing virtual currency because it imposes certain reporting requirements on the third parties employed by those users.

Specifically, as an MSB, any virtual currency administrator or exchanger must register with the Treasury Department[11] and also must maintain a list detailing its agents.[12] Further, like all financial institutions under the BSA, virtual currency exchangers and administrators must obtain identifying information for participants in transfers of $3,000 or more.[13] As MSBs, they also must establish anti-money laundering (AML) programs designed to thwart money laundering and maximize compliance with all BSA duties.[14] Finally, individual users of virtual currency could be swept up by the BSA reporting requirements for suspicious activity reports (SARs), which certain financial institutions—including MSBs—must file to report known or suspected money laundering activity, BSA violations or other crimes.[15]

Nonetheless, effective reporting regimes depend on actual compliance. One may wonder how diligent many current administrators and exchangers of virtual currency will be in carrying out their obligations to register, file SARs and enforce AML programs, particularly if they entered virtual business precisely because of its perceived enhanced anonymity.

The Virtual Implications Of Reporting Requirements For Offshore Accounts

The government's effort to subject virtual currency systems to the regulatory regime of the BSA implicates another potential parallel between virtual currency and the offshore account enforcement campaign: the lurking issue—not addressed by the recent IRS guidance—of whether individuals possessing virtual currency may have to file an FBAR. The FBAR—an annual reporting form imposed by the BSA, not the tax code—has been the engine driving the government's enforcement campaign against undisclosed offshore accounts, including the associated voluntary disclosure programs and criminal cases. If the recent history of expanding regulation of virtual currency is any guide, the government may be looking to fit the peg of virtual currency into the hole of FBAR reporting requirements.

Very generally, the FBAR must be filed by June 30 with the Treasury Department by U.S. citizens and residents with a financial interest in, or signatory authority or other authority over, ''financial accounts'' located in a foreign country that have a combined value of more than $10,000 on any day during the prior calendar year.[16] Not filing a required FBAR, or filing a false FBAR, is a felony if done willfully.[17] Further, the civil penalties for ''willful'' FBAR violations are severe: a monetary penalty equal to 50 percent of the highest account balance during the year of violation, cumulatively assessed for up to six years.

FinCEN already has taken the first step toward applying FBAR obligations to virtual currency by declaring, as described, that an administrator or exchanger of virtual currency is a type of ''financial institution'' subject to the BSA. The main remaining questions appear to be whether a stash of virtual currency represents (1) a ''financial account'' (2) that is ''foreign'' under the FBAR regulations. The possible answers are unclear and may turn on the precise technology used by an individual, a scenario that suggests a kaleidoscope of potential reporting obligations.

FBAR Basics

The FBAR reporting requirement applies to certain types of ''accounts,'' all of which receive specific definitions. They are: ''bank'' accounts, ''securities'' accounts and ''other'' financial accounts.[18]

The third, ''catchall'' definition of ''other'' financial accounts is broad and includes insurance or annuity policies with cash value, mutual and similarly pooled funds, brokerage accounts and commodity futures or options accounts. Further—and most relevant to virtual currency—it includes ''an account with a person that is in the business of accepting deposits as a financial agency,''[19] which is someone ''acting for a person . . . as a financial institution, bailee, depository trustee, or agent, or acting in a similar way related to money, credit, securities, gold, or a transaction in money, credit, securities, or gold.''[20]

Given the broad interpretation of ''money'' FinCEN used when it declared that administrators and exchangers of virtual currency are BSA money transmitters, it is this last type of ''other'' financial account that may apply most easily to certain virtual currency holdings.

The definition of ''foreign'' is more straightforward. Reportable accounts for FBAR purposes involve only accounts located in geographical areas outside the U.S.,[21] although a branch of a foreign bank physically located in the U.S. does *not* qualify.

The Mechanics of Virtual Currency: A Reportable Foreign Account?

When determining whether this regulatory framework may apply to virtual currency, the particular technology chosen by a user of virtual currency is likely critical because it determines *how* and *where* the currency is stored. The following very general discussion is limited to how bitcoin, the most common virtual currency, works.

A bitcoin user needs to create a virtual ''wallet,'' which stores both:

[10] See FIN-2013-G001, supra.
[11] 31 C.F.R. § 1022.380(a).
[12] 31 C.F.R. § 1022.380(d).
[13] 31 C.F.R. § 1020.410.
[14] 31 U.S.C. § 5318(h); 31 C.F.R. § 1022.210. However, the general Customer Identification Program requirement of the BSA, 31 U.S.C. § 5318(l), which requires certain financial institutions to gather information on all prospective customers attempting to open accounts at the institution, does *not* apply to MSBs.
[15] 31 C.F.R. §§ 1021.320-1026.320; 1029.320.
[16] 31 U.S.C. § 5314; 31 C.F.R. § 1010.350.
[17] 31 U.S.C. §§ 5314, 5322.
[18] 31 C.F.R. § 1010.350(c).
[19] 31 C.F.R. § 1010.350(c)(iii).
[20] 31 U.S.C. § 5312(a)(1).
[21] 31 C.F.R. § 1010.350(d).

■ the private keys needed to access the user's bitcoin addresses and spend her bitcoins; and

■ the public addresses through which other people send bitcoins to the user.

To acquire bitcoins, one uses a public address to buy bitcoins or provides a public address to a third-party so that the bitcoins can be deposited into one's wallet. A user can have many different bitcoin addresses.

Once a bitcoin user creates her wallet, a transaction between two wallets is initiated by use of a private key, which tells the system that the user wants to transfer value to the other person. The private key acts as the sender's signature and provides mathematical proof that the message came from the actual owner of the wallet. The transaction is verified by a ''mining'' system using a ''block chain.'' Mining is the process of validating transactions; miners throughout the globe use special software to solve extremely complex math problems. The block chain is a shared public ledger that contains every transaction ever executed in bitcoin. Using the block chain, one could discover the transactions associated with a given address. In this way, the use of bitcoin is subject to tracing and is not truly anonymous, although an address—which is just a randomized line of numbers and letters—does not itself reveal the user's actual identity. The more addresses used by an individual, the more splintered will be her full digital trail.

Does a bitcoin wallet constitute a ''foreign account'' subject to FBAR reporting requirements? Perhaps. There are five main types of bitcoin wallets—some of which depend upon the physical presence of the virtual currency user herself.

Desktop Wallets: Wallets maintained on a desktop computer can conduct transactions, create addresses and store keys. The user has total control but also has total responsibility. If the computer is stolen or destroyed, so are the bitcoins.

Paper Wallets: These are simply paper documents that list the keys that comprise a wallet. Paper wallets also can have quick response codes, so they can be scanned to add keys into a software wallet. These wallets are not subject to hacking, but they are obviously subject to fire, water and being lost or stolen.

Hardware Wallets: A hardware wallet electronically stores keys offline; for example, it could include a USB drive. Hardware wallets dedicated to virtual currency are still rare and most are still in production. A fascinating example became available in February: a wristband that is dedicated to holding private keys and that relies on the user's heart rhythm as a security key. Hardware wallets generally present the same advantages and disadvantages of paper wallets.

Mobile Wallets: These wallets allow easy access to bitcoins. By running an application on a smartphone, the mobile wallet stores the private keys for bitcoin addresses and allows for the potential easy exchange of bitcoins through the scanning of a QR code. Mobile wallets use a simplified payment verification based on a small subset of the block chain.

Online Wallets: Online wallets store keys on a website controlled by a third party. These wallets allow access to bitcoins by signing into the website through any browser or mobile device. However, the website that hosts a user's bitcoins may lose (or steal) them. The most notorious example of online wallets is Mt. Gox, a defunct bitcoin exchange based in Tokyo. Mt. Gox, which once handled most bitcoin exchanges, announced in February that it was bankrupt and had lost—apparently due to hacking—approximately 850,000 bitcoins held in online wallets and worth hundreds of millions of dollars.[22] Although Mt. Gox recently announced that it located about 200,000 of the missing bitcoins, this catastrophe remains a strong cautionary tale.

Of the various options above, and depending on the facts, online wallets represent the most likely candidates for qualifying both as ''accounts'' and ''foreign.'' Here, the two issues tend to converge. Continuing to use Mt. Gox as an example, the government presumably would regard Mt. Gox as an MSB and therefore as a financial institution. Because the owner of the wallet could deposit, transfer and withdraw money from it, and also because the wallet would resemble traditional accounts in other ways (i.e., the user can access it with a username and password and carry a balance), the government also could regard the wallet as an ''account'' under the FBAR regulations. Given the location of Mt. Gox in Japan, it also would be ''foreign.''

The government recently has focused on similar issues when taking the position in a civil FBAR enforcement action, arguing that the defendant's online accounts at FirePay, PokerStars and PokerPlayer represented foreign financial accounts subject to FBAR reporting.[23] In that pleading, the government argued that the companies that operated the sites represented foreign financial agencies and emphasized that the defendant had a username and password login access to his online accounts, carried a balance in them and could deposit, withdraw and transfer money from them. Further, the companies were licensed, and had their physical offices located, abroad. It is not hard to conceive of the government taking similar positions as to online wallets.

However, the government (and individuals) may face a bewildering regulatory field in which reporting requirements turn on the particular technology at issue. For example, if a user of virtual currency in the U.S. simply holds his virtual currency on the desktop of his computer, smartphone, flash drive or other remote device and uses it to fund virtual transactions as desired, it is difficult to imagine how such holdings could represent ''foreign accounts,'' particularly because a mere user of virtual currency does not represent a financial institution.

Another potential wrinkle remains. Even if a person maintains his wallet remotely and in the U.S., the actual use of bitcoin requires entry into the Internet and mining through the block chain. The government might argue that because the block chain facilitates the transmission of funds, anything uploaded or mined through that site could represent a foreign account. However, FinCEN recently has ruled that, to the extent that a user creates or mines virtual currency solely for the user's

[22] 09 WCR 136 (3/7/14).

[23] *United States v. Hom*, No. 13-cv-03721, motion for summary judgment (N.D. Cal. April 14, 2014), available at https://docs.google.com/file/d/0B0SLTNWD-Z3YaHRJbzdPNnRsZ2s/edit?usp=sharing&pli=1.

   ISSN 1559-3185

own purpose, the user is not a money transmitter under the BSA.[24] Moreover, accurate FBAR reporting, which involves filling out a form that asks for specific high balances held at specific accounts in specific places at specific times, would be almost impossible as a real-world proposition because block chain transfers last for only about 10 minutes and can be mined by someone anywhere in the world, unknown to the user.

[24] FIN-2014-R001, *Application of FinCEN's Regulations to Virtual Currency Mining Operations*, available at http://www.fincen.gov/news_room/nr/html/20140130.html (Jan. 30, 2014).