taxnotes® international

Volume 91, Number 9 ■ August 27, 2018

U.S. Tax Implications of Cross-Border Cryptocurrency Bribes

by Selva Ozelli

Reprinted from *Tax Notes International*, August 27, 2018, p. 895

U.S. Tax Implications of Cross-Border Cryptocurrency Bribes

by Selva Ozelli

Selva Ozelli

Selva Ozelli is an attorney and CPA in New York.

In this article, the author examines the growing problem of cryptocurrency bribes — specifically cross-border bribes by U.S. multinational entities to foreign officials — and discusses the U.S. tax implications of these bribes.

The 2007-2008 global financial crisis brought new challenges for — and, in time, improvements to — the U.S. Foreign Corrupt Practices Act (FCPA) and its enforcement around the world. Over the last decade, the FCPA has been one of the most important tools in the worldwide effort to fight corporate bribery of foreign officials.

In the aftermath of the financial crisis — and at the urging of the G-20 — the OECD proposed tax transparency rules.[1] Since then, 147 jurisdictions have signed on to the OECD's Global Forum on Transparency and Exchange of Information for Tax Purposes and that effort has helped to improve the utility of the FCPA. It is increasingly common for heads of states, including royalty, to face prosecution and even jail time for transnational corruption-related offenses.[2]

The financial crisis also helped the crypto-economy emerge — enabling the cross-border, peer-to-peer transfer of value, including cryptocurrency bribes. In the crypto-economy, value can be created by mining, and distributed ledgers allow for the transfer of money over the internet without the involvement of banks, which must obey anti-money-laundering (AML) and know-your-customer (KYC) laws. Regulators and tax authorities are often unable to detect violations of the FCPA and tax laws. They are also often unable to detect money laundering or fraud that involves cryptocurrency.

Testifying before the U.S. Senate Subcommittee on Crime and Terrorism at a hearing led by Sen. Lindsey Graham, R-S.C., titled, "Protecting Our Elections: Examining Shell Companies and Virtual Currencies as Avenues for Foreign Interference," Scott Dueweke of DarkTower, a cybersecurity firm, explained:

> For cryptocurrencies, the greatest emerging threat of foreign funds reaching the coffers of political candidates, or to be used to fund other influence operations, are the increasing number and liquidity of privacy coins. These are cryptocurrencies that seek to evade efforts to identity their users through the blockchain, and criminals are using them. These funds do not need to stay in their virtual currency of origin, however. Digital money can be used through a huge matrix of exchangers. Thousands of them around the world — interconnected — and do not necessarily meet any type of KYC requirements. For somebody who knows what they're doing and is skilled, it's almost impossible to follow them through this matrix of exchangers.[3]

[1] Selva Ozelli and Roger Russell, "Is This Payment Reportable? Global Standard for Payment Disclosure," 2017 OECD Global Anti-Corruption & Integrity Forum (Mar. 2017).

[2] Ozelli, "Why Are Heads of State Facing More Enforcement Actions?" The FCPA Blog (Apr. 4, 2018).

[3] U.S. Senate Subcommittee on Crime and Terrorism, "Protecting Our Elections: Examining Shell Companies and Virtual Currencies as Avenues for Foreign Interference" (June 26, 2018).

This article explores the U.S. tax implications of cryptocurrency bribery payments made by multinational entities in violation of the FCPA. It is a follow-up to an earlier article by this author, which provides useful background information on the FCPA and other applicable U.S. tax laws.[4]

I. Cryptocurrencies and Bribery

On the heels of the financial crisis, a programmer (or group of programmers) in Japan using the pseudonym Satoshi Nakamoto launched the groundbreaking bitcoin blockchain network, releasing the first units of the bitcoin cryptocurrency (BTC) on January 9, 2009.[5] Nakamoto intended the system to reduce fraud — the root cause of the financial crisis.

Blockchain technology permits users to transfer value person-to-person — including across borders — over the internet. It records and verifies every transaction chronologically and publicly, guaranteeing the integrity of financial records and making the falsification or destruction of the records practically impossible. The technology greatly reduces the potential for errors reconciling complex and disparate information from multiple sources, and it does not allow users to retroactively alter records.

Vitalik Buterin, the creator of Ethereum, a second-generation blockchain, has said:

> All transactions under Blockchain come with auditable trails of cryptographic proofs. Rather than simply hoping that the parties we interact with behave honorably, we are building Blockchains that inherently build the properties in the system, in such a way that they will keep functioning with the guarantees that we expect, even if many of the actors involved are corrupt.[6]

Blockchain technology and cryptocurrencies has become one of the most talked-about topics among global intergovernmental organizations, regulators, legislators, central bankers, and G-20 world economic leaders. These varied groups agree that cryptocurrencies and blockchain technology — a new class of digital asset with a borderless, intangible nature — are fundamentally reshaping global cross-border financial connectivity and increasing the ability to automate cognitive tasks.[7] In July, following a meeting that addressed a range of issues including cryptocurrency, the G-20 finance ministers and central bank governors released a communique stating:

> Technological innovations, including those underlying crypto-assets, can deliver significant benefits to the financial system and the broader economy. Crypto-assets do, however, raise issues with respect to consumer and investor protection, market integrity, tax evasion, money laundering and terrorist financing.

Further, cryptocurrency's privacy features facilitate cross-border crimes.[8]

Transactions that occur on a blockchain must follow the protocols that the computer programmer who developed the blockchain has set, not the rules set by a judge or a judicial body. Buterin explains:

> For example, you can't say in cryptoeconomics, "It's illegal to bribe people," because there's really no simple way to define what a bribe is. If someone really wants to bribe someone else, he can just go and do that outside of the protocol, and the protocol would have no way to tell.[9]

Scholars from the University of Sydney, the University of Technology Sydney, and the

[4] Ozelli, "Is This Bribe Deductible? Tax Implications of the U.S. Foreign Corrupt Practices Act," *Tax Notes Int'l*, Dec. 17, 2007, p. 1171.

[5] Ozelli, "Bitcoin and Solar Energy Fuel Investment in Japan: Expert Take," Cointelegraph (Feb. 28, 2018).

[6] Ozelli, "Smart Contracts Are Taking Over Functions of Lawyers: Expert Blog," Cointelegraph (Jan. 12, 2018). *See also* Ozelli, "Why Canada Has Emerged as a Leading Blockchain and Crypto Nation: Expert Take," Cointelegraph (Apr. 29, 2018); and Ozelli, "Canada (Yes, Canada) Focuses on Blockchain to Fight Graft," The FCPA Blog (Jan. 30, 2018).

[7] Ozelli, "Latest Pronouncements From OECD, EU & G20 Allow Fintech to Flourish: Expert Take," Cointelegraph (Mar. 26, 2018).

[8] Ozelli, "Illicit Uses of Cryptocurrency Gaining Attention Around the World: Expert Take," Cointelegraph (Feb. 20, 2018); and Ozelli, "'Mixing Services' Shield Cryptocurrencies and Thwart AML Practices," The FCPA Blog (Feb. 19, 2018).

[9] Akash Anand, "Ethereum [ETH]'s Vitalik Buterin Speaks: Cryptoeconomics, Blockchain and Their Future," AMBCrypto (July 19, 2018).

Stockholm School of Economics in Riga agree. Introducing a paper they released in February, the researchers state:

> We find that illegal activity accounts for a substantial proportion of the users and trading activity in bitcoin. For example, approximately one-quarter of all users (25 [percent]) and close to one-half of bitcoin transactions (44 [percent]) are associated with illegal activity. Furthermore, approximately one-fifth (20 [percent]) of the total dollar value of transactions and approximately one-half of bitcoin holdings (51 [percent]) through time are associated with illegal activity.[10]

In the context of the FCPA, examples of this illicit activity and the features that enable it include:

- *Person-to-person*: Relying on cryptography, MNEs can transfer digital cryptocurrency bribes person-to-person across multiple borders, moving funds from one country to the next beyond the purview of regulators.
- *Anonymity*: MNEs can conceal illicit activity — including bribery, money laundering, and tax evasion — by using cryptocurrencies that feature varying levels of anonymity and pseudonymity.
- *Mining*: MNEs can obtain cryptocurrencies to use for bribes to foreign officials by mining. They can create cryptocurrency privately — even on their smartphones — without the involvement of centralized issuers. However, the absence of centralized issuers with a mandate to guarantee the stability of cryptocurrencies renders their value unstable.
- *Storing*: MNEs can store intangible cryptocurrencies in various wallets. AML and KYC laws do not apply, and these wallets fall outside the control of regulators, allowing the MNEs to conceal illicit activities that extend into multiple countries around the world.

However, MNEs should carefully consider the FCPA, money laundering, fraud, and tax penalties — both civil and criminal — that could soon become a core focus of regulatory enforcement in the cryptocurrency space. The Department of Justice, the SEC, and the IRS — the groups that enforce the FCPA in the United States — have appointed their first cryptocurrency czars: Michele Korver,[11] Valerie Szczepanik,[12] and John Cardone.[13]

II. Cryptocurrency Bribes and U.S. Tax Law

In the United States, the Financial Crimes Enforcement Network, the Office of Foreign Assets Control, the IRS, the Commodity Futures Trading Commission, and the SEC are all involved in regulating cryptocurrencies at the federal level. The first two entities characterize cryptocurrency as money, while the remainder classify them as property, commodities, and securities, respectively.[14] The different classifications of cryptocurrencies create uncertainties regarding the U.S. taxation of cryptocurrency and blockchain technology transactions — and industry participants are eagerly awaiting answers and clarification.

Regardless, digital currency fraud will be one of the areas that a new U.S. anti-crime task force — a group that will involve several U.S. government bodies including the Department of Justice, SEC, CFTC, and the Treasury Department — will focus on according to the "Executive Order Regarding the Establishment of the Task Force on Market Integrity and Consumer Fraud" that President Trump issued on July 11.

A. Deductibility of a Cryptocurrency Bribe

1. Treatment of Cryptocurrency

Improper payments made in cryptocurrencies by an MNE — especially those involving

[10] Sean Foley, Jonathan R. Karlsen, and Tālis J. Putniņš, "Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies?" (Jan. 15, 2018).

[11] Ozelli, "Meet DOJ's Crypto Czar," Cointelegraph (July 23, 2018).

[12] Kirill Bryanov, "What Do We Know About Valerie Szczepanik, the First Crypto Czar," Cointelegraph (June 12, 2018).

[13] IRS, "IRS Announces the Identification and Selection of Five Large Business and International Compliance Campaigns" (July 2, 2018).

[14] Ozelli, "Sanctions Compliance For Transactions in Fiat And Cryptocurrencies Are The Same: Expert Take," Cointelegraph (Apr. 13, 2018); and Ozelli, "ICOs Flow Continues As Regulations Fall Around the World: Expert Blog," Cointelegraph (Nov. 26, 2017).

"cryptocurrencies with anonymity features [that] impede investigations of flow of money which in turn allows illicit transactions to occur outside of the regulatory perimeter"[15] — are not allowable expense deductions when calculating a company's worldwide profits and earnings under generally accepted accounting principles. This is because — despite its name — cryptocurrency is not treated as currency under the current U.S. accounting framework. Cryptocurrency is not cash, currency, or a financial asset. Instead, accounting firm PwC believes that it should likely be accounted for as an indefinite-lived intangible asset and capitalized.[16]

The implication of this model is that declines in the extremely volatile market price of cryptocurrencies would be included in earnings, but neither increases in value beyond the original cost nor recoveries of previous declines in value would be captured. The Financial Accounting Standards Board is researching accounting for cryptocurrencies as it considers setting standards. Without clear U.S. accounting rules, identifying improper payments made in cryptocurrencies in an MNE's books and records could be challenging.

For U.S. tax purposes, the IRS treats cryptocurrency bribery payments as property under Notice 2014-21, 2014-16 IRB 938. An MNE should not claim cryptocurrency bribes as tax deductions on the company's tax returns under IRC section 162(c). On May 30, the American Institute of Certified Public Accountants sent a letter to the IRS — for a second time — asking for more direction on cryptocurrency taxation beyond Notice 2014-21.[17]

2. The New Bribe Scenario

Suppose a U.S. MNE bribes a foreign official with a ZTE phone that serves as both a cryptocurrency miner and a cryptocurrency wallet.[18] The foreign official can mine Ethereum (also known as ether, or ETH) as needed, store the ETH in a wallet, sell the mined ETH on a foreign crypto exchange, and submit a very large electricity bill to the MNE as reimbursement for mining activities — all in exchange for pursuing business in the foreign country.

This so-called new bribe eliminates the need for lawyers, accountants, bankers, consultants, and other middlemen — as well as the need for things like bank accounts, sham consultancy contracts, and undisclosed offshore intermediary entities. It also differs from the traditional FCPA bribery schemes that involve hidden slush funds denominated in fiat currencies.

Nevertheless, the new bribe involves something of value and appears to violate the FCPA. Further, if the MNE deducts the payment as a business expense for U.S. tax purposes under IRC section 162(c), the company is exposing itself to numerous fines and penalties.

It is worth taking a deeper look at how to value the new bribe based on AICPA's letter to the IRS. Users obtain ETH either by exchanging fiat currencies for ETH, by exchanging initial coin offering tokens for ETH, or by mining, which is the process of having computers compete to solve complex mathematical problems.

The response to question 8 in Notice 2014-21 states that when a taxpayer successfully mines virtual currency, "the fair market value of the virtual currency as of the date of receipt is includible in gross income." This implies that ETH mining is similar to a service activity. Therefore, the costs of mining virtual currency should be treated like expenses incurred in providing other services, which are expensed as paid or incurred.

The AICPA's letter contains language that the group recommends the IRS add to expand its guidance regarding virtual currency. It suggests treating cryptocurrency that a taxpayer obtains by mining as ordinary income in the year it is mined and allowing the taxpayer to deduct the expenses of mining as incurred. The AICPA argues that the matching of income and expenses is consistent with other service activities. Also, the letter suggests that any cryptocurrency mining equipment — like the ZTE ETH phone in our example — should be capitalized and depreciated, just like any other property with a useful life of over one year.

[15] Ozelli, Interview of Assistant U.S. Attorney Puneet V. Kakkar (July 10, 2018) (on file with the author).

[16] PwC, "Cryptocurrencies: Time to Consider Plan B" (Mar. 6, 2018).

[17] American Institute of CPAs, "Updated Comments on Notice 2014-21: Virtual Currency Guidance" (May 30, 2018). *See also* Ozelli, "Supplemental IRS Guidance on Taxation of Cryptocurrencies Is Needed: Expert Take," Cointelegraph (June 2, 2018).

[18] *See* Ozelli, "How Should Cryptocurrency Bribes Be Valued?" The FCPA Blog (July 12, 2018).

Some cryptocurrencies, including ETH, are traded on centralized exchanges operating outside the United States. The exchanges are either a pure virtual currency exchange or a virtual currency exchange that allows virtual currencies to be exchanged for fiat currencies. These foreign virtual currency exchanges have custody of their customers' virtual currencies — an exchange failure results in the loss of customer funds. Notably, the SEC recently addressed ETH specifically, characterizing it as a commodity and not a security.[19]

The AICPA's letter to the IRS suggests that taxpayers should report the value of cryptocurrencies and fiat currencies held at foreign exchanges for purposes of the Report of Foreign Bank and Financial Accounts and the Foreign Account Tax Compliance Act, assuming the taxpayers meet the necessary threshold. However, the letter does not call for reporting when a taxpayer holds cryptocurrency in a wallet — such as a ZTE ETH miner/wallet phone — which the taxpayer owns and controls and for which the taxpayer has a private key.

That reasoning suggests that a ZTE phone enabled for ETH mining and wallet functions given by an MNE as a new bribe to a foreign official has only the intrinsic value of the phone itself and nothing more.[20]

B. Bargain Sales of Cryptocurrencies

Other problems may arise when an MNE makes an improper payment to a foreign official using a cross-border "bargain sale" of a cryptocurrency — that is, either selling it for less than its FMV or at a loss.

For example, suppose the company owns ETH with a basis of $50 and a FMV of $100. If it sells the ETH to a foreign official at a bargain price of $70, the IRS would treat the company as if it had received the full appreciated value of the ETH in the sale — that is, it would have gross income of $50. However, the taxpayer would not be eligible for a corresponding section 162(c)(1) deduction for the bargain element of $30 because the taxpayer's payment would constitute an improper payment. If the company sells the same ETH to the foreign official for $35 and then claims a loss of $15 on the transaction under section 165, the IRS could disallow the loss using a public policy argument.

A cryptocurrency has an equivalent value in fiat currency or acts as a substitute for real currency based on its determinable value in the market.

As the AICPA explains:

> Section 4, Q&A-5 of Notice 2014-21 refers to exchange rates established by market supply and demand used to determine the fair market value of virtual currency in USD as of the date of payment or receipt. It also recommends that taxpayers use a "reasonable manner that is consistently applied" to calculate the fair market value of virtual currency.

The letter also suggests that "further guidance and examples are necessary to define 'reasonable manner'" since there could be considerable differences in cryptocurrency pricing among different exchanges. Further, the AICPA suggests that the IRS allow taxpayers to use an average of the values on different exchanges as long as they calculate the valuation consistently. Likewise, taxpayers should be able to choose either the specific identification or first-in, first-out method for calculating their cryptocurrency gains and losses as long as they do so consistently.

C. Cross-Border Taxes on Cryptocurrency Gains

When a company makes an improper cross-border payment to a foreign official in the form of a cryptocurrency, the payment has an equivalent value in fiat currency. Any U.S.-source gain on the conversion may be subject to a cross-border withholding tax that may be reduced or eliminated by a tax treaty.[21]

The code does not specify how to determine the source of each item of income, particularly a cryptocurrency gain. But it does enumerate specific types of income that are considered U.S.-

[19] Lucas Mearian, "SEC Official Says Ethereum Is Not a Security, Freeing It From Oversight," Computer World (June 14, 2018).

[20] Ozelli, "How Should Cryptocurrency Bribes Be Valued?" *supra* note 18.

[21] IRC section 863(e). *See also* Ozelli, "Virtual Currency: U.S. Tax Considerations and Fraudulent Activity Amid a Growing Global Market," *Tax Notes Int'l*, Oct. 16, 2017, p. 257.

source and offers examples of similar types of income that are treated as income from sources outside the United States. The code also recognizes that income may be sourced partly from within and partly from outside the United States.

Because sourcing rules apply to different types of income, proper income sourcing depends on proper characterization of gain on ETH transferred to the foreign official via the internet. The characterization of the ETH gain could be determined under the international communications source rules. International communications income includes all income from the transmission of communications or data from the United States to any foreign country (or U.S. possession), or from any foreign country (or U.S. possession) to the United States. It includes any transmission of signals, images, sounds, or data by cable or satellite, including cryptocurrencies that are no more than data (a unique string of letters and numbers).

The regulations provide that income from a communications activity is classified by identifying, to the IRS's satisfaction, two points between which the taxpayer bears the risk of transmitting the communication — or, here, the cryptocurrency. They treat communications between two points within the United States as entirely U.S.-source, even if they are routed through a satellite located in space. Similarly, income attributable to communications between two foreign locations is completely foreign-source. Thus, the rules would likely source cryptocurrency bribery payments to a foreign official as 50 percent U.S. income and 50 percent foreign income.

D. CbC Reporting of Cryptocurrency Bribe

1. Contents of Reports

U.S.-headquartered MNEs with annual revenues of at least $850 million must file U.S. country-by-country reports on Form 8975. They must disclose information regarding cryptocurrency bribery transactions to tax authorities on a CbC basis, including:[22]

- the legal name of the entity;
- tax jurisdiction and residence of the entity;
- the tax identification number of the entity;
- the main business activity or activities of the entity;
- total third-party revenue;
- total revenue generated from transactions with related parties;
- pretax profit and loss amounts;
- total income tax paid (including withholding tax);
- total current-year accrued income tax expenses (excluding reserves);
- stated capital;
- total accumulated earnings;
- total number of employees; and
- total net book value of tangible assets, which may include cryptocurrencies or cryptocurrency mining equipment because they are classified as property and not currency for U.S. tax purposes (cash or cash equivalents, intangibles, and financial assets need not be declared).

The U.S. will automatically exchange CbC reports with other governments in accordance with tax treaties and tax information exchange agreements.

2. Penalties

MNEs that fail to file a CbC report could be subject to penalties under U.S. federal tax rules or under the rules of the 57 other countries that have agreed to exchange CbC reports. Further, the U.S. Supreme Court said in *Pasquantino v. United States*, 544 U.S. 349 (2005), that federal wire fraud charges could be brought against violators of foreign tax laws.

E. Uncertain Tax Position Disclosures

1. Reporting Rules

Since tax year 2010, MNEs with year-end assets of at least $10 million have used Form 1120 Schedule UTP (Form 8886) to report UTPs using the financial reporting process detailed in the FASB's Accounting Standards Codification Topic 740, "Income Taxes Disclosure Framework." This provides MNEs with a mechanism to evaluate filing positions and compliance risks, which would include section 162 trade or business

[22] Ozelli, "Virtual Currency," *supra* note 21; and Ozelli and Russell, "Is This Payment Reportable?" *supra* note 1.

expense deductions for cryptocurrency bribes to foreign officials.

An MNE only files a Schedule UTP when the company records a reserve for a U.S. income tax position in its (or a related party's) audited financial statements or the corporation (or related party) did not record a reserve for that tax position because the corporation expected to litigate the position.[23] Schedule UTP requires taxpayers to disclose a concise description of each UTP and then rank them from highest to lowest by size of the position based on the federal income tax reserve amounts. Schedule UTP does not require the company to disclose the actual amounts of the reserves. The IRS has also stated that Schedule UTP disclosures are not intended to raise questions of waivers of privilege as to confidential communications regarding the disclosed tax positions.

2. Penalties

A corporation may have to pay a penalty if the rules require it to disclose a reportable transaction under section 6011 and it fails to properly complete and file Form 8886. Penalties may also apply under section 6707A if the corporation fails to file Form 8886 with its corporate return, fails to provide a copy of Form 8886 to the Office of Tax Shelter Analysis, or files a form that fails to include all the required information (or includes incorrect information). Other penalties, such as an accuracy-related penalty under section 6662A, may also apply.

III. Conclusion

The FCPA continues to celebrate its popularity among investigative bodies around the globe that are probing companies for the widespread corporate practice of making improper payments to foreign officials. In the future, these multijurisdictional investigations will likely include cryptocurrency bribery payments as well. Because of the cross-border nature of blockchain technology, it is likely to be multinational tax units or groups that will undertake these investigations, specifically recently formed groups focused on curbing tax evasion involving illicit digital financial flows like the J5 — an international tax unit consisting of departments and agencies from Australia, Canada, the Netherlands, the United Kingdom, and the United States[24] — and the BRICS countries (that is, Brazil, Russia, India, China, and South Africa).[25] ■

[23] IRS, "Uncertain Tax Positions — Schedule UTP." *See also* IRS, "Schedule UTP Filing Statistics" (Oct. 6, 2016); and Treasury Inspector General for Tax Administration, "The Uncertain Tax Position Statement Does Not Contain Sufficient Information to Be Useful in Compliance Efforts," 2018-30-023 (Mar. 23, 2018).

[24] Ozelli, "Global Regulators Join Forces to Combat Crypto Crimes," The FCPA Blog (July 9, 2018). *See also* Nana Ama Sarfo, "The J5 and International Tax Enforcement," *Tax Notes Int'l*, July 23, 2018, p. 331.

[25] Sarfo, *supra* note 24.