

depletion are. Here, it is critical not to mistake the legal form for the economic substance. For example, a rule that reduces your interest deduction by \$1 for every \$1 you spend on meals and entertainment does not have the economic effect of discouraging interest expense; it has the economic effect of discouraging meals and entertainment expenses. It matters not that the impact is accounted for on the interest line of the tax return. Similarly, switching to a rule that reduces your interest deduction by 30 percent of your depreciation allowance is economically equivalent to slower depreciation rules — the wrong direction if your goal is a cash flow tax.

George Callas
 Steptoe & Johnson LLP
 May 12, 2021



Withholding Tax Consequences of Extortion Payments in Bitcoin

To the Editor:

The weekend news reports regarding the cyberattack on the 5,500-mile Colonial Pipeline providing petroleum products to the eastern United States obviously involve issues of national security and disruption of the U.S. economy,¹ but they also concern a tax issue that the IRS ought to address.

As is typical of cyberattacks on U.S. infrastructure, hospitals, school districts, municipalities, and the like, the hackers responsible for the Colonial attack will require payment in Bitcoin or other virtual currency in order to remove the malware that prevents the attacked company's computer systems from operating.² The reason for the demand for Bitcoin or other virtual currency is the obvious one that the recipient of the payment cannot be identified.

The IRS has provided a reasonable amount of guidance to date regarding Bitcoin and other virtual currency transactions, and the practicing bar has requested additional guidance. But nothing to date addresses the treatment of extortion payments in these currencies, and yet this would seem an important area for guidance with the number and scope of these transactions expected to increase as large-scale attacks occur and substantial, anonymous ransom payments are successfully extracted.³

As is well known, Bitcoin and other virtual currencies have been highly controversial, not

¹Ken Dilanian and Kelly O'Donnell, "Russian Criminal Group Suspected in Colonial Pipeline Ransomware Attack," NBC News, May 9, 2021. According to one commentator, "'This could be the most impactful ransomware attack in history, a cyber disaster turning into a real-world catastrophe,'" said Andrew Rubin, CEO and cofounder of Illumio, a cybersecurity company."

²See Lauren Fedor, Myles McCormick, and Hannah Murphy, "Cyber Attack Shuts Major U.S. Pipeline System," *Financial Times*, May 8, 2021 ("The number of ransomware attacks has exploded in recent years as criminals have used cryptocurrencies such as Bitcoin to receive extortion payouts without being tracked, and have increasingly rented out their expertise to others."); see also McCormick et al., "U.S. Declares State of Emergency to Keep Fuel Flowing After Cyber-Attack," *Financial Times*, May 9, 2021.

³See Notice 2019-24, 2019-14 IRB 932, answers to frequently asked questions regarding Bitcoin and other virtual currencies. Q&A 13 notes that payments to an independent contractor in Bitcoin or another virtual currency are subject to information reporting under section 6041. See also New York State Bar Association Tax Section, "Report on the Taxation of Cryptocurrency," No. 1433 (Jan. 26, 2020).

only because of their obvious suitability for use in the black market, tax evasion, and criminal enterprises generally,⁴ but also because of the extreme electrical energy consumption necessitated by so-called mining transactions. Fully 0.68 percent of the world consumption of electrical energy is occasioned by Bitcoin⁵ — approximately equal to the electricity consumed by Argentina.⁶ The increased popularity of Bitcoin has dramatically increased its energy consumption since 2017.⁷

In terms of the ransom demanded by the Colonial Pipeline hackers, it seems plain that the extortion amount represents taxable income to the hackers,⁸ and that it is fixed and determinable annual or periodical income.⁹ Assuming that no information is reliably known regarding the identity of the hackers, their status as U.S. or foreign persons, or the source of the income that they earn — which likely will depend on where their extortion “services” are performed¹⁰ — consideration must be given to the applicable U.S. withholding tax requirements. Absent such information, it appears that the backup withholding regime will apply, necessitating withholding at a 24 percent rate. Variations regarding information concerning the hackers

might possibly implicate withholding at source at a 30 percent rate under chapter 3. The Treasury regulations, however, appear to favor domestic backup withholding under section 3406.¹¹ In any event, it would seem desirable for the IRS to promptly clarify this treatment given the apparent widespread practice of making these ransom payments in Bitcoin or other virtual currencies, and the expectation that the number and magnitude of the payments is likely to increase.

Very truly yours,

Richard L. Reinhold
Cornell Law School
May 9, 2021

■

⁴ In a similar context, the 1982 Tax Equity and Fiscal Responsibility Act eliminated the use of so-called bearer bonds — which were transferred by delivery alone and therefore facilitated criminal enterprises and tax evasion. See sections 149 (interest on state and local obligations in bearer form do not qualify for tax-exemption), 163(f) (denying interest deductions on bonds in bearer form), 165(j) (denying loss deductions for bearer bond transactions), and 4701 (excise tax on issuance of bearer bonds).

⁵ See University of Cambridge, “Bitcoin Electricity Consumption Index.”

⁶ See Digiconomist, “Bitcoin Energy Consumption Index.” For further perspective, a single Bitcoin transaction is estimated to produce 403.39 kg CO₂, which is equivalent to the carbon produced by 864,060 Visa transactions or 67,232 hours of YouTube videos.

⁷ *Id.* It also appears that a very significant portion of Bitcoin mining occurs in China with electricity being generated by burning coal, the most detrimental fuel in terms of the impact on the environment. See Jonathan Ponciano, “Crypto Flash Crash Wiped Out \$300 Billion in Less Than 24 Hours, Spurring Massive Bitcoin Liquidations,” *Forbes*, Apr. 18, 2021.

⁸ *Rutkin v. United States*, 343 U.S. 130 (1952).

⁹ See reg. section 1.1441-2(b)(1)(i).

¹⁰ Obviously, the hackers’ removal of the malware once the ransom has been paid is not a service in any conventional sense, but the sourcing rules for services would seem applicable by analogy. See *Bank of America v. United States*, 680 F.2d 142 (Fed. Cir. 1982). On the other hand, because the criminal activity involves hacking into software that is presumably protected under U.S. law, perhaps U.S. sourcing is more appropriate. Compare *Piedras Negras Broad. Co. v. Commissioner*, 43 B.T.A. 297 (1941), with section 861(a)(4).

¹¹ See reg. section 1.1441.1(b)(3)(ii)(B).