Ransomware and Bitcoin – Tax Troubles?

Feb 10, 2021

Categories:

Blogs
Tax Law Defined™ Blog

Authors:

Elizabeth M. Ethington
Mark F. Sommer

Published reports suggest that many businesses, including HBO, Xerox, Garmin, ExecuPharm and several hospital systems and local governments, have fallen victim to ransomware attacks. That is where a breach of cybersecurity leaves the business locked out of its networks until demanded payments, usually in the form of cryptocurrency such as bitcoin, are made. While a ransomware attack is a federal offense, the hassle and time constraints to override the breach often leave businesses weighing these concerns and ultimately finding it easier to make the payment and move on. However, in considering which path to take when faced with this issue, it is important for businesses to consider the tax and regulatory implications.

The first tax consideration is whether these payments are a cost of doing business and can be deducted from taxable income. One way a business could consider deducting these payments is as theft loss. IRC Sections 162(a) and 165(a) provide companies authority to deduct any losses that were not covered by insurance or some other means. There are several judicial and administrative definitions of theft, but the IRS's definition seems broad enough to encompass a cyber-attack. Pursuant to Revenue Ruling 72-112, 1972-1 C.B. 60, the IRS defines theft as an illegal taking of property with criminal intent to receive ransom for the return of the property. In PLR 7946010, the IRS applied this definition to a kidnapping, providing that ransom payments made in a kidnapping situation could be deducted.

While there has been no *official* federal guidance on this issue, there has been industry speculation that ransomware payments could be deducted for federal purposes as a business expense. In order to deduct these payments as a business expense, the payments must be considered "ordinary and necessary." While 10 years ago payment for a cyber-attack may not have been considered "ordinary," as more and more businesses fall victim to this type of activity, such payments could arguably fall under the U.S. Supreme

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

Court's definition of ordinary, meaning "normal, usual or customary." Additionally, if such payments are a means of unlocking a company's data and networks, ransomware payments arguably could be considered necessary for the continued operation of the taxpayer's business.

However, because *illegal payments are not deductible*, a taxpayer must be clear to differentiate ransomware payments. IRC 162(c) does not allow a deduction "if the payment constitutes an illegal bribe, illegal kickback, or other illegal payment under any law of the United States." This has judicially been expanded to include blackmail payments. Thus, in order to distinguish blackmail payments from ransomware payments, a taxpayer must highlight the theft of its property. Cyber-attacks are often not just threats but takings involving possession of property.

Because ransomware payments are often required to be completed in the form of cryptocurrency, another consideration for businesses is whether these payments subject the company to federal and state oversight or disclosure regarding cryptocurrency transactions. There are several federal agencies that monitor cryptocurrency exchanges. While the facts and circumstances of the transaction must be considered, the Securities and Exchange Commission (SEC) regulates any issuance or resale of any token or digital asset that creates a security, at times determining that certain digital assets are investment contracts. If this happens, the issuer must register the digital assets with the SEC. Some states also enforce such registration under their respective blue sky laws. But if one simply purchases virtual currency from a marketplace to make the payment, this is likely not a concern.

Additionally, the Financial Crimes Enforcement Network (FinCEN) also regulates the cryptocurrency space. In 2013, FinCEN issued a statement providing that "an administrator or exchanger that accepts and transmits a convertible virtual currency or buys or sells convertible virtual currency for any reason is a money transmitter." Thus, pursuant to the Bank Secrecy Act (BSA), FinCEN can regulate these transactions. Under the BSA, a cryptocurrency transmitter is required to complete a risk assessment, develop a written program to avoid money laundering, designate an individual compliance

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

officer, and complete other action items.

Lastly, in terms of the federal tax consequences of using cryptocurrency, the IRS has declared that virtual currency is taxed as property rather than currency. Specifically, taxpayers are expected to keep detailed records of cryptocurrency transactions, report any gains from cryptocurrency transactions for cash or for a good or service, and report the fair market value of any mined cryptocurrency. So, in the case of a ransomware payment in the form of cryptocurrency, the IRS could see this as a taxable transaction.

The IRS has greatly expanded its analysis of cryptocurrency since it announced its classification as property in 2013. The IRS now has on its website a page dedicated to virtual currencies and the various tax treatments thereof. This guidance includes items such as whether a taxpayer should recognize a gain or loss when selling virtual currency, tax treatment in the exchange of services for virtual currency, and other growing concerns for taxpayers using virtual currency. And on some tax compliance forms, the IRS is requiring each taxpayer to acknowledge owning or transacting in cryptocurrency. Thus, it is clear that the IRS is continuing to pay closer attention to such transactions and how taxpayers are accounting for them, or not, on their respective returns.

While many states are still struggling with what to do with blockchain technology – whether to regulate and enforce it or provide incentives to move more tech companies to its jurisdictions – using cryptocurrency to complete ransomware payments could have state tax implications as well. In addition to licensing requirements some states impose, other states have recognized sales and use tax liability for cryptocurrency exchanges. States such as California and Washington have expressed that they treat cryptocurrency exchanges the same as a typical sale of tangible personal property. Other states have decided to create carve-outs or specific rules to govern cryptocurrency exchanges.

When a business is faced with a network security breach and must decide whether to make a ransomware payment, it should consider all these aspects of federal and state regulation and tax

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

implications. For the latest in federal and state tax news, visit Frost Brown Todd's Tax Law Defined Blog.

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

FBT Gibbons