



Robert W. Wood

THE TAX LAWYER

TAXES 12/08/2016

Prosecutors Pay Bitcoin Ransom, Yet IRS Targets Coinbase Data

In the midst of the IRS's [legal battle](#) to uncover the identities of Bitcoin users, federal prosecutors have revealed that a state prosecutor's office had to battle for its own private information, also involving Bitcoin. Pennsylvania's Allegheny County District Attorney's Office apparently paid a [Bitcoin ransom](#) to protect the privacy of its *own* information. The amount of the ransom was relatively small, [only \\$1,400](#) in good old dollars. But it's still remarkable seeing a government entity paying a *ransom*, and even more so in a digital currency such as Bitcoin.

One can imagine that some Coinbase users would gladly pay a ransom (if they could) to avoid the IRS finding them, and auditing them! Then we could talk about whether paying ransom should be tax deductible as a business expense. In this case, though, it was the *government* paying ransom. One wonders if this was all some kind of retaliation.



Shutterstock

After all, though markets suggest that [Bitcoin is expected to surge 165% thanks to Donald Trump](#), the IRS is still playing hardball. The IRS's recent summons to Coinbase is about getting at some coveted anonymity. In fact, though, the ransom comes from a widespread phishing attempt, not one that targeted the DA's office specifically. Moreover, the goal seems to have been profit, not ideology.

Nevertheless, it is interesting to consider both sides of this (Bit)coin. The hackers, known as the Avalanche Group, presumably demanded to be paid in Bitcoin because payments in the digital currency can be much harder to trace than transactions involving the banking system. (Well, for now.) Even if the IRS does get its hands on the Coinbase user data, including names and addresses of people who bought and sold Bitcoins, it still may have a very hard time tracing these transactions to unreported income and taxable transactions.

Still, the IRS's crackdown on digital currencies is [just beginning](#). Users should be wary, and most importantly, should plan ahead. The IRS's efforts toward offshore account disclosure enforcement also started on a small scale. In fact, the IRS started out [with just one bank](#): UBS AG. The government's focus then turned to other Swiss banks, and eventually to banks all around the globe that were hiding U.S. taxpayer's funds. So, Coinbase may be the tip of the iceberg too.

In the offshore account mess, [tens of thousands of taxpayers came forward](#) through the various iterations of the IRS amnesty programs. In general, those who did so early got better deals. And those who came late or took no action faced higher penalties, or even criminal investigations. In October of 2016, the IRS said its [offshore account collections topped \\$10 billion](#). And it still isn't over yet.

Now, it seems to be the turn of digital currency users to watch the IRS gear up. We should expect that the government will get what it wants in the end. Just about everything is income to the IRS. If you suspect you might need to clean up past tax filings, or just want to fly right in the future, don't wait. That's especially true of more serious cases. If you fear that you may be at risk of a criminal investigation, you may want to consider [how to establish attorney-client privilege with your accountant](#).

That way you can have a bit more security as you consider amending past returns to include payments received in digital currencies. The same is true of filing information reporting returns such as Forms 8938 or FBARs.

Businesses may need to file the [necessary Forms 1099](#) for payments to independent contractors made in digital currency, or Forms W-2 for payments to employees.

And back to Bitcoin ransoms. If you end up paying one, can you claim it as a tax write-off? Maybe so. The IRS says a [“kidnapping for ransom” can qualify as a deductible theft](#), as does blackmail, embezzlement, and extortion. However, as with all deductions, you need to keep your receipts, and your Bitcoin transaction logs. From that viewpoint, you might actually want to hang onto those ransom letters.

For alerts to future tax articles, email me at Wood@WoodLLP.com. This discussion is not legal advice.