Hogan Lovells

IRS Renews Focus on Cryptocurrency-Related Offenses

August 2019

The Internal Revenue Service (IRS) has signaled for years that it would eventually bring enforcement actions against individuals who failed to report cryptocurrency gains. It appears that "eventually" is over and that those actions are underway.

Late last month, news reports indicated that the IRS had begun sending letters to individuals who engaged in virtual currency transactions. In late July, the IRS issued a news release stating that, by the end of August, more than 10,000 taxpayers will receive one of three "educational letters" in order to "help taxpayers understand their tax and filing obligations and how to correct past errors."[1] And, just last week, it was reported that the IRS was putting increased pressure on certain taxpayers by sending another round of letters (called CP2000 Notices) to individuals whose reported information did not match information provided by third parties.[2]

What does all of this mean in terms of IRS enforcement? There are several key takeaways.

A focus on criminal enforcement: While the IRS itself characterized the three versions of its letter as "educational," that is only partly the case.[3] One version of the letter (Form 6173) appears to reflect the agency's preliminary belief that taxes are owed – potentially as a result of something other than a misunderstanding. In that letter, the IRS declares that the taxpayer "may not have met your U.S. tax filing and reporting requirements for transactions involving virtual currency."[4] Notably, this letter does not contain the same "educational" material included in the other two, but instead extends an invitation

[1] *See* https://www.irs.gov/newsroom/irs-has-begun-sending-letters-to-virtual-currency-owners-advising-them-to-pay-back-taxes-file-amended-returns-part-of-agencys-larger-efforts.
[2] *See* https://www.irs.gov/individuals/understanding-your-cp2000-notice.
[3] It is true that one version of the letter explains that the IRS has "information that you have or had one or more accounts containing virtual currency but may not know the requirements for reporting transactions involving virtual currency." *See* https://www.irs.gov/pub/notices/letter_6174.pdf. The second version goes a little further, explaining that the taxpayer "may not have properly reported [] transactions involving virtual currency." *See* https://www.irs.gov/pub/notices/letter_6174-a.pdf. In both, the IRS includes educational material, including information regarding the proper reporting of virtual currency transactions.
[4] *See* https://www.irs.gov/pub/notices/letter_6173.pdf.

to the taxpayer to explain why he or she "followed all tax and information reporting requirements relating to your virtual currency" with an accompanying declaration under penalty of perjury.

This letter appears to be in line with the IRS's news release, which makes reference to criminal enforcement three times in just over 350 words. The news release states that "[v]irtual currency is an ongoing focus area for IRS Criminal Investigation [IRS-CI]" and "[i]n some cases, taxpayers could be subject to criminal prosecution." So while the IRS is certainly using these letters at least in part to "educate" taxpayers regarding their reporting obligations, the message in general is that the IRS stands ready to prosecute cases.

Continuation of IRS's recent focus on cryptocurrency: IRS-CI has been focused on cryptocurrencies for some time now, and has been building its momentum ever since a critical report from the Treasury Inspector General for Tax Administration in September 2016.[5] It has been just over a year since the IRS created the Joint Chiefs of Global Tax Enforcement (J5), a coalition between five countries (the United States, Australia, Canada, the Netherlands, and the United Kingdom) aimed at investigating cryptocurrency crimes, including tax fraud and money laundering. The stated purpose of the J5 is to "gather information, share intelligence, conduct operations and build the capacity of tax crime enforcement officials."[6]

Earlier this year, the IRS deployed data analytics and technology-based programs through the creation of a nationally coordinated investigations unit (NCIU). On March 8, 2019 at a Federal Bar Association conference in Washington, Don Fort, the head of IRS-CI, said that the NCIU would be focused on tax cases involving cryptocurrencies, and he was quoted as saying "[w]e're already in the process of building models in that area and have already had some preliminary success in identifying some areas of noncompliance there."[7] He added, "[w]e're just scratching the surface."

Further, Fort has repeatedly stated over the last year that digital currencies were an area of focus for his special agents. In IRS-CI's 2018 annual report, Fort touted the agency's ability to investigate significant cybercrime cases – referencing enforcement actions against digital currency companies Liberty Reserve and BTC-e – and he stated that "[w]e now require all CI employees—not just special agents—to complete cyber training."[8]

And, just last week, at the largest anti-money laundering casino conference in the country, Fort again stressed his agency's attention and expertise around cryptocurrencies.

Preparing for investigations: Although to date there have been only a handful of criminal enforcement cases involving cryptocurrencies, IRS-CI has been investing time to train its special agents in anticipation of an uptick in enforcement, as reflected in IRS-CI's 2018 annual report. Last month it was revealed that the IRS-CI Cyber Crimes Unit, which was created in 2015, has been training special agents about the

---

[5] *See* https://www.treasury.gov/tigta/auditreports/2016reports/201630083fr.pdf.
[6] *See* https://www.irs.gov/compliance/joint-chiefs-of-global-tax-enforcement.
[7] *See* https://www.taxnotes.com/tax-notes-federal/criminal-violations/federal-bar-association-section-taxation-irss-data-driven-tax-enforcement-approach-here-stay/2019/03/18/297df?highlight=referrals%20and%20double%20and%20fort%20and%20cryptocurrencies%20and%20models.
[8] *See* https://www.irs.gov/pub/irs-utl/2018_irs_criminal_investigation_annual_report.pdf.

ecosystem and technology underlying cryptocurrency markets, such as blockchain, exchanges, and wallets, as well as the top cryptocurrencies (including Bitcoin, Ethereum, XRP, Bitcoin Cash, Litecoin, Stellar, and Monero).

The training also involved the various ways to gain information about cryptocurrency users, including methods such as scanning social media sites and issuing grand jury subpoenas to banks and technology companies (when applications owned by those companies transmit or allow cryptocurrency transactions). The use of grand jury subpoenas is notable because IRS-CI special agents do not possess the authority to issue grand jury subpoenas.[9] Instead, IRS-CI must first request that (a federal prosecutor (often from Department of Justice's (DOJ) Tax Division) opens a grand jury investigation).[10]

The important sub-text regarding the use of grand jury subpoenas is that IRS-CI almost certainly has ongoing grand jury investigations alongside the Department of Justice Tax Division or one of the United States Attorney's offices.

What happens next?

If you were one of the recipients of these letters, it does not necessarily mean that you owe taxes. But for those recipients who do in fact owe taxes, these letters serve an important enforcement purpose other than "educating" you on your obligations.

In a criminal tax prosecution, the government must prove that the taxpayer willfully violated the tax laws, which is a higher standard than in most white collar criminal prosecutions. To prove willfulness (in the criminal context), the government must establish that the taxpayer was actually aware of his or her obligations under the tax laws. The IRS appears well aware that cryptocurrency users could otherwise claim ignorance of the law based on developing and often conflicting regulatory requirements, and these letters were almost certainly intended by the IRS to counter a potential ignorance defense. As such, it is possible that this letter-writing campaign could be tied to several high-profile individual prosecutions, and these letters would certainly be part of the evidence the government would argue established willfulness.

Moreover, while the IRS indicated in its news release that it identified the recipients of these letters "through various ongoing IRS compliance efforts," the identities were likely obtained, at least in large part, from the IRS's highly public action against Coinbase, the digital currency wallet and platform. That is also certainly true regarding the CP2000 Notices.

In the Coinbase matter, IRS-CI and DOJ sought and obtained a *John Doe* summons, which is a powerful enforcement tool that, if approved by a federal court, allows the IRS to obtain from a financial institution or other organization the names and requested information and documents concerning all taxpayers in a certain group. In this matter, IRS-CI obtained information on all accounts with transactions greater than $20,000, which amounted to more than 13,000 users. That data was turned

[9] Typically, and especially in more traditional tax investigations (like underreporting of lawful income and employment tax violations), IRS-CI special agents initiate a criminal investigation using administrative tools, such as witness interviews, open source records, and administrative subpoenas.

[10] *See* Justice Manual §§ 6-4.110, 6-4.120, and 6-4.120, available at https://www.justice.gov/jm/jm-6-4000-criminal-tax-case-procedures.

over to the IRS in early 2018, and the IRS has been mining that trove of data against tax returns to determine which users reported taxable earnings and which did not.

Notably, the tactics in the Coinbase matter mirror those used by the IRS and DOJ to pierce the veil of Swiss banking secrecy over a decade ago in the UBS case. In that case, a *John Doe* summons was approved by a federal court in 2008, and it took years for the IRS and DOJ to review that data and make subsequent enforcement decisions. If the UBS case and the larger Swiss Bank Program[11] presage anything about the current environment, it would be that cryptocurrency exchanges and platforms should expect the enforcement drumbeat to continue for years – even if the enforcement priority is at the moment focused on individuals and not the exchanges and platforms themselves (although that is less than clear at the moment).

Why should cryptocurrency exchanges and platforms expect this level of scrutiny?

It is because the IRS thinks it has a massive problem on its hands. As such, this will remain a focus area for IRS-CI for years to come.

Contacts

David Sharfstein
Counsel
Washington, D.C./Baltimore
T +1 202 637 5739/+1 410 659 2721 E
david.sharfstein@hoganlovells.com

Gregory Lisa
Partner
Washington, D.C./New York
T +1 202 637 5910 / +1 212 918 3644
gregory.lisa@hoganlovells.com

[11] The Swiss bank program was formally announced on August 29, 2013 and provided a path for Swiss banks to comply with U.S. law and resolve potential criminal liabilities.