THE
NATIONAL LAW REVIEW

Digital Cops and Cyber Robbers: OFAC Guidance on Crypto Currency

Thursday, April 12, 2018

A lot of us in the sanctions compliance world were wondering whether and when OFAC would issue official guidance on its application of sanctions in the digital currency world. On March 18, OFAC issued five FAQs related to virtual currency. Those FAQs convey two important messages:

(1) OFAC sanctions regulations apply to virtual currency transactions just as they apply to "fiat" currency (here's looking at you dark web crypto-user); and

(2) OFAC will use its existing authority to respond to the growing threat posed by the use of emerging payment systems by malicious actors, including adding digital currency addresses that are associated with blocked persons to the SDN List.

SheppardMullin

Article By
Fatema K. Merchant
Sheppard, Mullin, Richter & Hampton LLP
Global Trade Law Blog

Antitrust & Trade Regulation
Communications, Media & Internet
Financial Institutions & Banking
All Federal

While the first point – that OFAC compliance obligations apply to virtual currency transactions – is not groundbreaking news, the second point is more interesting. Our key takeaway from the FAQs is: OFAC is clearly thinking about how it will enforce its regulations on virtual currency transactions and digital currency operators, so you should too.

OFAC Compliance in Virtual Currency Transactions

In general, U.S. persons and persons subject to OFAC jurisdiction are prohibited from engaging in unauthorized transactions that are unlawful under OFAC sanctions regulations, including dealings with blocked persons or property or prohibited trade or investment-related transactions subject to country-specific sanctions. As FAQ 560 points out, "prohibited transactions include transactions that evade or avoid, have the purpose of evading or avoiding, cause a violation of, or attempt to violate prohibitions imposed by OFAC under various sanctions authorities."

Regulating in the Dark: What is Unclear About Cryptocurrency Sanctions Policy

As OFAC and the rest of us regulatory types get our heads around the technology and industry of virtual currencies, we are simultaneously grappling with how to help clients involved in those emerging technologies comply with the existing regulations. Regulations are generally developed with mature industries in mind. So, as emerging technologies create brand new industry models, applying those existing regulations feels like trying to fit a square peg into a round hole . . . while the hole is changing shape . . . and new holes are being created all around.

OFAC regulations are implemented through a complicated web of statutes, executive orders, regulations, general licenses, interpretive guidance documents, and yes, even answers to FAQs. Even for industries that are more traditional and well-developed, with robust internal infrastructure – accounting departments, lawyers, compliance personnel, real names and addresses of customers – compliance with OFAC regulations can be tricky. So OFAC is likely still struggling to understand how it will issue meaningful guidance for virtual currency players, how it will identify potential violations, and thus, how it will investigate potential violations and enforce its regulations.

Shedding a Little Light: What is Clear About Cryptocurrency Sanctions Policy

But the FAQs that OFAC issued make clear that the agency expects "technology companies; administrators,

exchangers, and users of digital currencies; and other payment processors" to develop "tailored, risk-based" compliance programs related to OFAC sanctions regulations. OFAC does not provide much detailed guidance on those programs, but states that they should include sanctions lists screening and "other appropriate measures."

If you're in the virtual currency business or just a "user" of digital currency, you should be thinking about how to develop a risk-based sanctions compliance program (if you haven't already done so) that is effective and practical for your business. Most companies use screening software or other automated platforms for sanctions screening, but given that the identities of virtual currency users are anonymous by design, conducting diligence to ensure that they are not transacting with prohibited parties in virtual currency transactions will require some creativity.

OFAC's Strategies to Enforce Sanctions Regulations: Adding to the SDN List

Shedding a Little Light: What OFAC Intends to Do

OFAC plans to use sanctions to combat the global threat of "malicious actors abusing digital currencies and emerging payment systems" in addition to the existing diplomatic and law enforcement tools. One of the strategies OFAC is considering is to "include as identifiers on the SDN List specific digital currency addresses associated with blocked persons." OFAC will identify the digital currency addresses on the SDN List by the unique alphanumeric identifiers (up to 256 characters) and the digital currency to which the address corresponds ((e.g., Bitcoin (BTC), Ether (ETH), Litecoin (LTC), Neo (NEO), Dash (DASH), Ripple (XRP), Iota (MIOTA), Monero (XMR), and Petro (PTR)).

Regulating in the Dark: OFAC is Learning and So Are We

OFAC acknowledges that the list OFAC will generate is "not likely to be exhaustive" and persons who identify wallets that they believe to be owned by or are associated with blocked persons an SDN should block relevant digital currency and file a report with OFAC. "Associated with" is not defined. Therefore the scope of digital wallets potentially covered by sanctions is expansive. First, OFAC's "50% rule" instructs that a blocked person is considered to have an interest in all property and property interests that the person owns, whether individually or in the aggregate, directly or indirectly, of 50% or more. It is unclear how OFAC will apply the 50% rule and how OFAC interprets the term "associated with" in the digital wallet context.

Several other questions remain regarding the regulations, such as the following:

1. How, in practical terms, virtual currency recipients are expected to block transactions;
2. Whether all customers of a multisig wallet provider or custodial exchange will be subject to regulatory requirements if that wallet or exchange is listed;
3. How OFAC will track certain sanctioned users given the reality that wallet addresses can be changed and that many addresses are single-use; and
4. How OFAC will track the actual identity of address users (because the mapping between users and public key addresses will be challenging, to say the least).

What we do know is that if you engage in a prohibited transaction that violates country-specific sanctions or deals with a blocked person, the stakes are high. A violator is subject to significant criminal and civil penalties, and risks being designated on the SDN list itself under applicable OFAC authority.

There will certainly be uncertainty as OFAC deepens its understanding of the cryptocurrency industry and as the industry learns how best to comply with the existing regulatory framework. During that time, companies and individuals engaging in digital currency transactions should invest smart compliance resources into assessing their risks and understanding how the government intends to enforce its complex and constantly changing sanctions laws. That will help those companies and individuals reduce their potential criminal and civil exposure. We will keep you updated as we learn more.