Despite growing scrutiny and enforcement in the cryptocurrency space, regulatory uncertainty remains

As the world marks the eleven-year anniversary of the seminal Satoshi Nakamoto white paper, which introduced the world to Bitcoin, the cryptocurrency industry remains a relatively nascent, highly volatile, somewhat untrusted, and uncertain industry. Despite – or to spite – the statements of certain regulatory and law enforcement agencies, virtual currencies do not neatly fit into existing regulatory structures. Depending on the specific circumstances, crypto-assets may be regulated by any of a number of federal agencies within the United States (not to mention the array of state or foreign agencies who might stake a claim to jurisdiction). The process of applying a complex network of laws and rules enforced by different agencies onto these new technologies, products, and services has resulted in an opaque regulatory environment. This in turn yields reluctance to provide investment for much-needed research and development, along with genuine uncertainty as to how to comply with an evolving regulatory landscape.

The uncertainty starts with the question of which regulatory agency has jurisdiction over these products and businesses. Various agencies – the Commodity Futures Trading Commission (CFTC), the Securities and Exchange Commission (SEC), and the Financial Crimes Enforcement Network (FinCEN) – have all asserted some form of oversight and regulation over this industry, proliferating the space with enforcement actions, speeches, guidance, and advisories, as well as other public-facing statements regarding virtual assets. On October 11, 2019, the leaders of these respective agencies issued a *Joint Statement on Activities Involving Digital Assets ("Joint Statement")* regarding the anti-money laundering obligations of those engaged in virtual currency.

The *Joint Statement* is certainly helpful in establishing that, because the Bank Secrecy Act (the principal U.S. anti-money laundering statute) applies to various types of financial institutions, including money transmitters, commodities brokers and futures commission merchants, and securities brokers and dealers, near-identical AML regulations apply regardless of the classification of the digital asset involved. At the same time, the joint guidance reiterates that a virtual asset's taxonomy is a function of "facts and circumstances underlying an asset, activity or service, including its economic reality and use (whether intended or organically developed or repurposed)". This strongly signals that subsequent use or market conditions could alter regulatory obligations and classifications, irrespective of developer (or creator or investor) intentions, leaving jurisdictional/regulatory interpretations fully open and somewhat unpredictable. Indeed, despite this coordinated announcement in the agencies' *Joint Statement*, it is not guaranteed that these agencies would necessarily defer to the others' respective interpretations or agree as to the scope of the others' jurisdictions.

Despite this lack of clarity, enforcement – theoretically predicated on the wrongful (and sometimes knowing and intentional) violation of clear, known (or at least knowable) rules – remains on the rise. For example, the SEC took action against the former owner of EtherDelta, a decentralized cryptocurrency exchange, for allegedly operating as an unregistered national securities exchange. According to the SEC, the platform facilitated secondary market trading of ERC20 tokens, a type of blockchain-based token commonly issued in Initial Coin Offerings. The matter was settled with neither an admission nor a denial of the SEC's findings, leaving unresolved the underlying question of whether the tokens were securities.

The jurisdiction of the CFTC with respect to cryptoassets extends to those that are commodities and not securities. While certain federal courts have found that cryptocurrencies are potentially commodities under the Commodity Exchange Act (CEA), commodity status for a specific cryptocurrency is still a fact-based, evolving analysis based on several factors, including how the cryptocurrency was issued, the purpose and use, the governance and degree of decentralization, and how the cryptocurrency was promoted. Recently, the CFTC Chairman stated that Ether, like Bitcoin, will be deemed a commodity regulated under the CEA. And even more recently, in late October, the Chairman posited that a digital asset might transform from a commodity to a security, or the other way around.

FinCEN, a bureau within the U.S. Department of the Treasury, administers the Bank Secrecy Act (BSA). Determining the applicability of its regulations to various cryptoassets may also be challenging as some decades-old regulations are applied to innovative products. The status of some actors in this space as "money transmitters" – a type of financial institution covered by FinCEN's rules – is the result of a facts-and-circumstances specific analysis that may provide only limited insight for purposes of future products. FinCEN has addressed how its money services business (MSB) regulations apply to business models for transactions involving convertible virtual currencies (CVCs), but any guidance applies only to that specific business model. Terminology and labels cannot easily be extended to other business models without a clear assessment of the underlying facts.

FinCEN's application of the regulations in the civil enforcement context has highlighted some of these issues and underscored the fact-specific nature of the analysis. In one enforcement action, FinCEN concluded that an operator was not merely a "user" of virtual currency (which would be outside of its jurisdiction), but rather a peer-to-peer exchanger of convertible virtual currency. As such, the operator was deemed a money transmitter and thus a financial institution for purposes of the anti-money laundering regulations and therefore subject to FinCEN's regulatory oversight. The operator was found to have

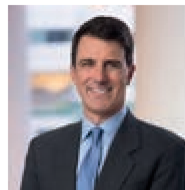
willfully violated the BSA's registration, program, and reporting requirements and accepted a civil monetary penalty. Other companies and individuals have likewise found themselves liable, and despite extensive guidance (most notably FinCEN's May 9, 2019 Advisory titled *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies)*, several open questions remain.

Complicating things further, cryptocurrencies and other virtual currencies are increasingly implicated in criminal activity. Despite their extensive legitimate uses, digital currencies have also been connected to narcotics trafficking, human trafficking, sanctions evasion, and terror finance, along with a whole host of other criminal activities. Money transmitting businesses and kiosks have been used to exchange millions in cash and virtual currency for criminals, including Darknet drug dealers. Criminal enforcement matters involving cryptocurrency include fraudulent conduct, especially (though not exclusively) related to the misrepresentation of assets underlying the value of tokens in connection with initial coin offerings and similar financing schemes that involve virtual currencies or other tokenized assets.

As cryptocurrencies grow in availability and prominence, regulators are responding to the potential use of cryptocurrencies to obscure identities and to conceal the origin, control, and source of assets. The Treasury Department's Office of Foreign Assets Control (OFAC) publishes the names of parties that are designated under a sanctions program and added to OFAC's list of "Specially Designated Nationals" or "SDN List." The assets of SDNs are blocked (frozen) and U.S. persons generally are prohibited from dealing with them. To address the possibility that U.S. persons could inadvertently transact with SDNs using cryptocurrencies, OFAC has included cryptocurrency addresses with the identifying information in certain designations.

On the taxation front, the Internal Revenue Service (IRS) has sent letters reminding certain taxpayers of the tax and filing obligations associated with virtual currency transactions. To prove willfulness in the criminal context, the government must establish that the taxpayer was actually aware of the obligations under the tax laws; the letters could potentially be used to establish such awareness. So while "educational," issuing the letters suggests a possible willingness by the IRS to prosecute cases. In early October, the IRS updated its draft tax return form (Form 1040) to ask filers whether they received, sold, sent, exchanged, or otherwise acquired any financial interest in virtual currency.

As industry attempts to navigate the complex U.S. regulatory map for cryptocurrencies, the risk remains that the uncertain regulatory environment will stifle innovation, discourage promising use cases for crypto-assets, and allow unsuspecting participants to unintentionally run afoul of the law. The cryptocurrency industry's ability to develop products that fit within a certain predictable regulatory framework will remain challenging as the law, policymakers, and markets attempt to keep up with and develop approaches to these innovative products and services.



Gregory Lisa
Partner, Washington, D.C., New York
T +1 202 637 3647 – Washington D.C.
T +1 212 918 3644 – New York
gregory.lisa@hoganlovells.com

Andrea Fraser-Reid
Knowledge Lawyer, Washington, D.C.
T +1 202 637 3676
andrea.fraser-reid@hoganlovells.com