wiley

ARTICLE

Regulatory Scrutiny Exposes Crypto Oversight Challenges

Law360
October 4, 2019

In the last few months, Congress has increasingly focused on the regulatory framework around wider consumer use of cryptocurrencies for payments — notably holding a pair of high-profile hearings in mid-July around the proposed Libra cryptocurrency.

In particular, the U.S. House Committee on Financial Services held a hearing on Sept. 24, with the commissioners of the U.S. Securities and Exchange Commission, during which Financial Services Committee Chairwoman Maxine Waters, D-Calif., pointedly noted that the new cryptocurrency must be "appropriately and rigorously regulated."

The announcement of a number of ambitious plans for widespread consumer use of crypto payments has led to a closer look at how cryptocurrencies might be regulated as a consumer financial product. Early innovators in this space, however, have been dealing with how to navigate existing consumer financial rules — which are not always a good fit for the technology. As crypto payments expand and policymakers look on warily, it's worth looking more closely at the regulatory challenges that companies face in this area.

Challenges in Moving Crypto Into Financial Services

In the early parts of the decade, cryptocurrencies — and Bitcoin in particular — were often discussed as potential payment mechanisms. Cross-border transactions were (and still are) cited as promising use cases where crypto technologies could make transactions cheaper and more efficient and directly benefit consumers.

Authors

Duane C. Pozza
Partner
202.719.4533
dpozza@wiley.law

Practice Areas

Privacy, Cyber & Data Governance

As long ago as 2014, the New York Department of Financial Services introduced licensing of cryptocurrency companies, the BitLicense, in anticipation of greater use of cryptocurrencies in financial services. Wider adoption has often been slowed by regulatory challenges that include securities, anti-money laundering and anti-terrorism requirements, but the Libra announcement illustrates the progress that many crypto innovators have made in making crypto financial services more mainstream.

Even without further congressional or regulatory action, these companies face regulatory and compliance challenges.

Fragmented Regulatory Structure and Ambiguous Definitions

Crypto innovators operating outside the bank regulatory space must deal with a wide range of governmental entities that may directly regulate their services, or scrutinize them under consumer financial services or other laws. Companies can face scrutiny from the Federal Trade Commission, the U.S. Consumer Financial Protection Bureau, state attorneys general and state financial services regulators, not to mention Congress.

In addition, questions remain about whether cryptocurrency is legal tender, money or a medium of exchange, as defined under state money transmitter laws. As a general matter, in most states, a money transmission license is required to engage in the business of receiving money for transmission.

While the NYDFS has introduced the BitLicense, at least one state financial services regulator, the Pennsylvania Department of Banking and Securities, has taken the position that cryptocurrency business operators are not required to apply for a money transmission license. According to the department, under Pennsylvania law only lawful money of the United States (i.e., currency issued by the U.S. government) is considered money in Pennsylvania.

Although no jurisdiction in the United States has designated virtual currency as legal tender, some state money transmission laws require licensure even where the medium of exchange is not legal tender. In Virginia, for example, a money transmission license is required to engage in the business of selling or issuing stored value. Monetary value is defined as a medium of exchange, whether or not redeemable in money. "Medium of exchange" is not defined expressly under Virginia law.

Companies face challenges in a number of areas.

Consumer Understanding and Disclosure Requirements

Tech innovators in the crypto space have a deep understanding of how the technology works and the potential risks that might come with using cryptocurrencies — potential price volatility and security, for example. But broader adoption of cryptocurrencies will bring many customers with no knowledge about how the underlying tech works or any potential pitfalls.

While many innovators are trying to make cryptocurrencies easier to use and to solve for potential problems — for example, taking steps to control for price volatility — they still must effectively communicate any material parts of transactions to consumers.

If consumers don't understand an important component of the transaction and suffer some kind of financial injury, regulators will be skeptical. For example, the FTC brought and settled an enforcement action against the operator of a popular peer-to-peer payment app alleging that the app informed consumers that they had received money that could be transferred out to a bank account, yet was deceptive because it failed to disclose that the funds could still be frozen or the transaction reversed.

Consumers may not understand how financial apps actually work, and companies must be careful in how they describe them. And notably, under deception law, law enforcers and regulators generally look at the least sophisticated reasonable consumer when evaluating consumer understanding.

Dealing With Fraud on a Decentralized Network

Cryptocurrencies are designed to operate on a decentralized blockchain. But as the technology has developed, innovators have come forward with intermediate entities like wallets or exchanges that deal with crypto assets, as well as crypto projects with more developed governance protocols. Innovators in this space cannot assume that the decentralized nature of cryptocurrencies also defuses potential liability. The more control a company exerts, either in terms of providing wallet or storage services or in controlling the protocol behind the cryptocurrency, the more that regulators and plaintiffs' lawyers will look for someone to be held liable.

This is particularly the case where regulators perceive there are high levels of fraud on a platform. In 2018, for example, the FTC and Department of Justice reached a $125 million settlement with MoneyGram International Inc., based on allegations that the company failed to prevent fraud through its services.

This followed a separate settlement with nearly all the state attorneys general and the District of Columbia, also based on third-party fraud. And the FTC has brought numerous cases against smaller companies it alleged knowingly processed fraudulent payments or consciously avoided knowing that the payments were unauthorized.

Moreover, companies operating a wallet, exchange or similar services may wish to provide voluntary fraud protections in order to promote consumer trust in the product. In 2016, the CFPB declined to explicitly extend Regulation E, which requires certain remediation in case of unauthorized transfers, to cover cryptocurrencies, but it remains possible that a regulator could attempt to enforce it in the context of crypto transactions.

But even voluntary consumer protections can be a potential pitfall, as regulators will attempt to hold companies to those representations. For example, the FTC sued a prominent prepaid card provider for

allegedly failing to timely provide provisional credits while investigating account errors, which was a voluntary policy by the provider.

Companies Face Tension Between Privacy Protections and Asset Security

Financial services companies run sophisticated fraud detection systems often built on extensive analysis of consumer data. Consumers expect banks or credit card companies to flag transactions that seem out of the ordinary based on how the consumer account is normally used.

But what about a cryptocurrency integrated into a social network? What kind of information is appropriate to use for safeguarding financial transactions, and, conversely, what kind of transaction information is appropriate to use for other services?

Other than the Gramm-Leach-Bliley Act, in general there are few mandatory restrictions on the use of consumer data by crypto companies under federal law. Companies will be held to their representations about how they use or transfer any data collected, and can be subject to an FTC or state enforcement action for failing to do so. And at the same time, companies are generally required to take reasonable data security measures by the FTC and states — a requirement that could well extend to protecting, for example, a consumer's private keys for their cryptocurrencies.

Regulators also may conclude that the more specific provisions of the GLB Act and its implementing rules may apply. For example, the FTC recently alleged a service provider to be a covered financial institution for purposes of the GLB Act's Safeguards Rule, based on a regulatory provision that sweeps in entities that engage in data processing services involving financial, banking and economic data.

While the agency has cited the data processing provision of the GLB Act before, its application in that case suggests the FTC could potentially attempt to sweep in many companies that may not otherwise consider themselves covered financial institutions. And the FTC is currently proposing revisions to add requirements to the Safeguards Rule, suggesting that it could be a renewed tool for enforcement.

In all of these areas, crypto companies' precise obligations may be unsettled under black-letter law. Companies must be prepared to deal with potentially shifting expectations that can emerge when legislators and regulators bring greater scrutiny. Crypto innovations hold enormous promise to improve financial services for consumers, but innovators will need to be mindful of how consumer regulations may be applied and take steps to address them in advance.