Crypto Exchanges Could Be Next Regulatory Target

Law360, (October 2, 2018)

Sarah Aucterlonie

Rikard Lundberg

Emily Garnett

On Sept. 18, 2018, the office of the New York state attorney general, or OAG, released the Virtual Market Integrity Report, a 40-plus page report on the state of crypto or virtual currency exchanges. Generally, exchanges serve as marketplaces to permit consumers to trade virtual currencies and may function similarly to traditional stock exchanges or broker-dealers.

To date, much of the regulators' attention has been on initial coin offerings, or ICOs. As regulators have broadened their expertise in virtual currencies and dedicated more resources to policing the industry, they have expanded their focus beyond ICO fraud and other ICO violations to the businesses behind post-ICO trading. The report indicates that regulators are now focused on more systemic issues, such as cybersecurity, preventing conflicts of interest, and market manipulation.

The report could thus serve as a warning to virtual currency exchanges that regulators may seek to impose requirements for traditional exchanges on virtual currency exchanges. Failing to heed this warning will likely lead to regulatory scrutiny, enforcement actions and consumer litigation. Moreover, as investors become more discerning about their preferred trading platforms, ensuring that an exchange has a sophisticated cybersecurity, monitoring and compliance protocol will serve as a market differentiator in the competitive virtual currency marketplace.

Below, we summarize a few key aspects of the report and provide a series of recommendations based on the report to serve as a quick reference guide to exchanges, their counsel and their customers.

Overview of the Report

The New York State Department of Financial Services, or DFS, and the OAG have been at the forefront of regulating virtual currency businesses. Exchanges that operate in New York must navigate a regulatory obstacle course to obtain a "BitLicense," New York's license for virtual currency businesses to operate in the state. DFS has approved few applicants, making BitLicense holders part of an exclusive club.[1]

Meanwhile, New York has cultivated one of the nation's most informed groups of regulators on virtual currency. To that end, in April 2018, the OAG commenced a fact-finding inquiry into the policies and practices of virtual currency exchanges to better inform the public and fellow regulators of the inherent risks and shortcomings of market-leading exchanges. The OAG submitted letters and voluntary questionnaires to 13 exchanges.[2] Notably, three exchanges (Binance, Gate.io and Kraken) refused to participate.[3] The OAG has since referred them to DFS to investigate potential violations of New York's virtual currency

regulations.

The OAG's questions covered five principal topics:

1. Jurisdiction, acceptance of fiat currency, and fee disclosures;
2. Trading policies and market fairness;
3. Management of conflicts of interest;
4. Security, insurance and protection of customer funds; and
5. Access to customer funds, suspensions and outages.

Based on the questions posed and the report's summary of those responses, we make a series of recommendations discussed below.

1. Exchanges should adopt robust customer verification and monitoring policies to identify customers and prevent money laundering.

In the earlier days, exchanges and regulators were more focused on preventing nefarious money laundering. Early congressional hearings on the industry focused on the risk that virtual currencies and their associated platforms would serve as a conduit for dark money transactions by drug dealers and terrorists. Many early industry leaders believed that having robust know your customer (KYC) and anti-money laundering (AML) policies satisfied their compliance obligations.[4] Although dark money still remains a risk and KYC and AML policies continue to be a pillar of any compliance regime, the report notes that verification of customers' identity and location is also important to ensure the fairness and integrity of the marketplaces.

One challenge in that regard is that users may access exchanges through virtual private networks, or VPNs, a tool designed to obfuscate a user's IP address. Notably, the report notes that only two of the nine survey respondents (Bitstamp and Poloniex, operated by Circle) have platforms that actually limit VPN access.

Based on the report, we recommend exchanges adopt policies and procedures to verify customers' identity and location. In particular, exchanges should consider whether to restrict VPN access or relatedly, consider what additional information must be provided in order to prevent circumventing one-user/one-profile requirements. Such policies will not only help prevent money laundering, but will also assist exchanges in preventing market manipulation, discussed in more detail below.

2. Exchanges should ensure that they adequately disclose all user fees and that their fees do not favor one investor over another.

Exchanges make money off of charging customers fees on their virtual currency transactions. The report describes that some exchanges do this on a flat-rate model while others adopt fee schedules based on the size or type of transaction. For example, some exchanges have the "maker-taker" model, whereby they impose higher fees on takers or customers who fill orders and lower fees on those that offer or "make" available an order for sale. The report also notes that many exchanges have hidden or nonobvious charges, such as charges for depositing or withdrawing customer virtual currency funds. Excessive or

hidden fees have been the source for dozens of lawsuits against traditional broker-dealer firms, serving as a warning sign to virtual currency exchanges.

Based on the report, we recommend exchanges adequately disclose all fees to avoid accusations of misrepresentation. Ideally, such fees should be disclosed multiple times to an investor — including disclosing the fees in any terms and conditions included in the user agreement, as well as disclosing the fees on the exchange's website and/or platform. Customers should be required to provide multistep or multiclick authorization of customer fees and should agree to submit any dispute regarding the exchange's fees to arbitration.

3. Exchanges should adopt policies aimed at promoting market integrity and preventing market manipulation.

The report notes that virtual currency exchanges operate without the regulatory oversight that traditional trading markets are subject to and that customers have less transparency as to how the exchanges operate and how to effectively participate in trading activities. This subjects customers to additional market integrity risks when compared to traditional trading markets.

Such risks include professional traders who employ sophisticated trading strategies to arbitrage market pricing gaps. These strategies include coordinating large bulk orders to push up the price of a virtual currency, as well as so-called "fill or kill" orders across multiple platforms, which are canceled if a bulk order is not placed in full. Professional, high-volume traders may also seek to "co-locate" or "cross-connect" their computers directly with an exchange's data center to ensure that their orders are placed as efficiently as possible without informational delays. More troubling, some professional traders have been cited for using computer-automated or "bot" training strategies, whereby they use programs to artificially move the price of a virtual currency in connection with their trading strategies.

Such practices may harm traditional retail virtual currency investors. The report focuses on the failure of exchanges to address these practices. Notably, only one exchange has implemented strategies to monitor and limit message rates among users (often a predecessor sign of market coordination and manipulation). The report further notes that at least one exchange (Bitfinex) allows users to place a "hidden" order that does not appear on publicly visible order books, potentially providing a price advantage to professional traders who can place sizable bulk orders without detection.

Based on the report, we recommend that exchanges adopt policies and procedures that define, detect, prevent and penalize suspicious trading activity and market manipulation to help protect the integrity of their trading platforms for traditional retail investors. Since this has been an area of frequent litigation in the traditional broker-dealer space, virtual currency exchanges can look to these businesses as guides for compliance protocols and policies. In this regard, the report notes that one respondent, Gemini, has partnered with Nasdaq to develop more sophisticated market surveillance tools and at least one other platform was in the process of contracting for a similar service. Because sophisticated users may attempt to manipulate the market across multiple platforms, exchanges should explore opportunities to coordinate monitoring with other platforms to ward against such manipulative activity.

4. Exchanges should ensure that employees are not trading based on insider trading

or otherwise engaging in conduct that is not in the best interests of its customers.

Managing conflicts of interests has long been a challenge for traditional financial institutions. In the virtual currency industry, this challenge is heightened by the thousands of virtual currencies available to the public and the lack of robust and systematic disclosures about each currency. As a result, exchanges serve as a gatekeeper to retail investors, and investors may come to trust the value of a currency because it is listed on a particular exchange. This gatekeeping function can lead to problems when exchanges do not disclose why they made certain currencies available on their platform over others. In fact, some exchanges receive kickbacks or special bonuses for promoting such listings. Such special benefits should be disclosed so that investors can incorporate that information into their investing decisions.

Further complicating investor protections, the report notes that many exchanges engage in their own proprietary training, whether through trading as an institution or by allowing employees to trade.[5] This creates additional risk that liquidity in the traded virtual currencies may change without notice and that exchanges and employees will trade on insider or nonpublic information.

Given these risks, we recommend that exchanges develop policies and procedures that address the following:

- Adopt standards for deciding whether a virtual currency should be listed on the exchange;
- Address employee and company proprietary trading; and
- Disclose compensation received for listing certain currencies.

Again, these issues have been the source of litigation against traditional broker-dealers and these lawsuits and their post-litigation policies and procedures can serve as a guide for content.

Exchanges should also ensure that such disclosures are regularly updated and monitored through planned audits of employee trading practices. This is particularly important when an exchange has a proprietary token that may be bought and sold by employees. In that regard, exchanges can look to public company guidance for preventing employees from selling and purchasing company stock based on insider information. We may eventually see the equivalent of so-called “10b5-1 plans,” named after a Securities Exchange Act of 1934 rule enacted as a safe harbor from the prohibition on insider trading, which sets out a preset schedule for trading stocks, thus eliminating the risk that trades are executed based on insider information.

5. Exchanges should continue to adopt policies and procedures that protect customer funds and ensure against losses.

Unlike the other topics discussed in the report, this is a topic that the virtual currency industry has long been focused on. High-profile hacking reports have sent warning signs to the industry to ensure protection of customer funds, which is a critical component of any

successful exchange. Because of unique features of virtual currency, such as the storage of an asset's "private key," this industry faces more complicated cybersecurity logistics than traditional exchanges.

As a result, the OAG sought confirmation that exchanges provide a two-factor authentication for customers at a minimum, which requires users to input both a password and another source of authentication (e.g., a code sent to a user's cellphone). It follows that this protocol should be incorporated into any exchange's compliance suite.

The OAG also focused on whether respondents obtained insurance to protect customer funds. Insurance has been notoriously difficult for many exchanges to obtain, largely because the traditional insurance industry has not yet developed an industry standard for quantifying risk. Notwithstanding such challenges, new insurance companies are moving into this space and should help fill the gap.

In addition to guidance distilled from the report, we recommend virtual currency exchanges work with third-party vendors to develop a comprehensive cybersecurity plan, conduct audits in connection with the plan, and make this plan available to customers with a waiver disclaiming liability. We anticipate an increase in customer litigation against exchanges in the event of a hack. Through investor education, the exchanges can go a long way at preventing hacks.

6. Exchanges must adopt policies that address trading outages and suspensions.

Industry leaders such as Coinbase have experienced outages due to heavy customer traffic and trading volumes. These outages can harm retail investors who are seeking to place orders and are prevented from taking advantage of dips or increases in virtual currency prices. The report notes that such delays may not always be based on high demand. Indeed, in such a highly technical and virtual space, exchanges frequently upgrade their system through daily scheduled maintenance or otherwise. In other cases, transactions may take minutes or even hours[6] to process, increasing the risk of delayed, suspended or inadvertent duplicate orders.

Based on the report, we recommend exchanges not only develop policies that set forth protocols for market outages and suspensions, but also address ways to educate customers about the risks of such outages and how the exchange intends to address them. Such considerations should discuss whether and how a platform will inform customers of these delays and if customers can still withdraw funds during this period.

In addition to implementing appropriate protocols, we recommend exchanges make robust, plain-English disclosures to the customer base in their user agreement's terms and conditions. Exchanges should educate customers about the risk of such outages and each firm should outline how it intends to provide best execution of trades notwithstanding.

Conclusion

The report serves as an important road map to virtual currency exchanges and their partners on future areas of regulatory scrutiny. Even for exchanges that have no intention of serving customers in New York, they would be well-served by studying the report and taking

into account the report's key findings when creating policies and procedures. As the virtual currency regulatory landscape continues to evolve, New York will undoubtedly be a leader in shaping that evolution.

Sarah Auchterlonie is a shareholder at Brownstein Hyatt Farber Schreck LLP. She is a former attorney with the U.S. Department of the Treasury's Office of Thrift Supervision and a former acting deputy enforcement director with the Bureau of Consumer Financial Protection's Office of Enforcement. She is also a current member of the Colorado Banking Board.

Rikard D. Lundberg is a shareholder and Emily R. Garnett is an associate at Brownstein Hyatt.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] Recently, DFS approved two more BitLicense applications reportedly bringing the total number to 11. See "DFS Continues to Foster Responsible Growth in New York's Fintech Industry with New Virtual Currency Product Approvals," (Sept. 10, 2018) available at: https://www.dfs.ny.gov/about/press/pr1809101.htm (noting two more product approvals); and "DFS Grants Virtual Currency License to Square" (June 18, 2018) available at https://www.dfs.ny.gov/about/press/pr1806181.htm (noting nine total approved licensees).

[2] The 13 exchanges were Bitfinex (operated by iFinex Inc.), bitFlyer USA Inc., Bitstamp Ltd., Bittrex Inc., Coinbase Inc., Gemini Trust Co., itBit (operated by Paxos Trust Co.), Poloniex (owned by Circle Internet Financial Ltd.), and Tidex (operated by Elite Way Developments LLP), HBUS (partnered with Huobi Inc.), Binance Ltd., Gate.io (operated by Gate Technology Incorporated), Huobi Global Ltd., and Kraken (operated by Payward Inc.).

[3] Kraken has since responded and noted that it voluntarily responded and informed the OAG that since it does not operate in NY it did not believe it was under an obligation to respond. "Coinbase and Kraken Push Back on OAG Report," (Sept. 20, 2018) available at https://www.ethnews.com/coinbase-and-kraken-push-back-on-new-york-oag-report.

[4] Indeed, many felt that such policies were overboard and a violation of the virtual currency culture, which was rooted in the concept of anonymity.

[5] The report noted that 20 percent of Coinbase's trades were connected to proprietary trading. In a response, Coinbase's chief policy officer denied that Coinbase engages in proprietary trading. See his response, "Correcting the record: Coinbase does not engage in proprietary trading," (Sept. 20, 2018) available at https://blog.coinbase.com/correcting-the-record-coinbase-does-not-engage-in-proprietary-trading-97e66145af6e.

[6] Steve Buchko, "How Long Do Bitcoin Transactions Take?" (Dec. 17, 2018) available at https://coincentral.com/how-long-do-bitcoin-transfers-take/; see also Block Trading Time

Chart, Bitinfo, available at https://bitinfocharts.com/comparison/ethereum-confirmationtime.html (last viewed Sept. 22, 2018).