Español

A.G. Underwood Issues Virtual Markets Integrity Report, Finding Many Platforms Vulnerable To Abusive Trading, Conflicts Of Interest, And Other Consumer Risks

Report and Interactive Website Outline What Cryptocurrency Platforms are Doing – and Not Doing – to Protect Retail Customers from Theft, Fraud, and Abuse

NEW YORK – Attorney General Barbara D. Underwood today announced the results of the Virtual Markets Integrity Initiative, a fact-finding inquiry into the policies and practices of platforms used by consumers to trade virtual or "crypto" currencies like bitcoin and ether.

The **Virtual Markets Integrity Report** released today, along with a user-friendly interactive website at **virtualmarkets.ag.ny.gov**, presents information collected by the Attorney General's office from 10 virtual asset trading platforms based in the United States and abroad, as well as the conclusions reached by the Attorney General's office about the state of the virtual trading markets as a whole. The Attorney General's office has also referred three platforms – Binance, Gate.io, and Kraken – to the New York State Department of Financial Services for possibly operating unlawfully in New York.

"New Yorkers deserve basic transparency and accountability when they invest – whether on the New York Stock Exchange or on a cryptocurrency platform. Yet, as our report details, many virtual currency platforms lack the necessary policies and procedures to ensure the fairness, integrity, and security of their exchanges," said **Attorney General Underwood**. "With this report, we hope to give New Yorkers the tools they need to make educated decisions on whether to entrust their money to a cryptocurrency platform and to help protect themselves against theft, fraud, and abuse."

Background

In April 2018, the Attorney General's office sent letters to thirteen major virtual currency trading platforms requesting key information on their operations, internal controls, and safeguards to protect customer assets. The Virtual Markets Integrity Initiative sought to increase the transparency and accountability of platforms that retail investors rely on to trade virtual currency, and to inform enforcement agencies, investors, and consumers.

The Attorney General's office asked the platforms to disclose information on six major topics, including (1) Ownership and Control, (2) Basic Operation and Fees, (3) Trading Policies and Procedures, (4) Outages and Other Suspensions of Trading, (5) Internal Controls, and (6) Privacy and Money Laundering. In particular, the Attorney General's office asked the platforms to describe their approach to combating suspicious trading and market manipulation; their policies on the operation of bots; their limitations on the use of and access to non-public trading information; and safeguards to protect customer funds from theft, fraud, and other risks.

Today's report informs the public about the Initiative's key findings, and educates consumers about the risks and protections available at the major virtual currency trading platforms.

Key Findings

The report details how virtual asset trading platforms vary significantly in the comprehensiveness of their response to the risks facing the virtual markets and fulfilling their responsibilities to customers. The Initiative also revealed three broad areas of concern for the virtual markets as a whole:

1. Lack of Protection from Abusive Trading Practices

The report finds that virtual asset trading platforms have yet to implement serious efforts to monitor and stop abusive or manipulative trading. Few platforms seriously restrict, or even monitor, the operation of "bots" or automated algorithmic trading on their venue. On the contrary, most platforms seem to cater to professional, automated traders – with many venues offering special pricing and other features to such traders, leaving retail customers at a disadvantage. For instance, some platforms offer high-speed direct market data feeds to professional traders; some permit traders to "co-locate" or "cross-connect" their trading computers to the platform's servers; and several offer so-called "maker-taker" pricing models. Those fee structures and services are designed to allow professional traders to leverage access and speed to power sophisticated automated trading strategies – strategies that can negatively affect the trading performance of everyday, non-automated customers.

2. Pervasive Conflicts of Interest

The report finds that virtual asset trading platforms engage in multiple, overlapping lines of business that present serious conflicts of interest. Customers need to understand whether and how trading platforms address these conflicts, and how platforms protect everyday traders from consequent disadvantage. Notably:

- Several platforms trade for their own account, on their own venue, in volumes that constitute a significant portion of total trading. This subjects everyday retail traders to the risk of illiquidity during times of price movement, and calls into question the true amount of natural liquidity on those venues.
- Several platforms allow their own employees to trade on their venue, and differ in their efforts to ensure that those employees do not use non-public information to gain an advantage over other traders.
- A few platforms issue their own virtual currencies or accept compensation in exchange for listing a virtual asset to trade. There are often no objective standards for listing particular virtual currencies, leaving serious questions about the elevation of particular virtual currencies over others on certain venues.

3. Limited Protection of Customer Funds

Generally accepted methods for auditing virtual assets do not exist, and trading platforms lack a consistent and transparent approach to independently auditing the virtual currency purportedly in their possession; several do not claim to do any independent auditing of their virtual currency holdings at all. That makes it difficult or

impossible to confirm that platforms are responsibly holding their customers' virtual assets as claimed. If a hack or unauthorized withdrawal occurs, customers are also highly exposed. There is no public protection (like FDIC insurance) to cover virtual currency losses, and there are serious questions about the scope and sufficiency of the commercial insurance that some platforms carry to cover those losses. Some platforms do not insure against virtual asset losses at all.

Questions Customers Should Ask Platforms

The report identifies several fundamental areas for customers to understand before trading on a virtual currency trading platform. In particular, the report cautions customers to be wary of any platform that cannot, or will not, answer the following questions:

1. What security measures are in place to stop hackers from unlawfully accessing the platform or particular customer accounts?

2. What insurance or other policies are in place to make customers whole in event of a theft of virtual or fiat currency?

3. What guardrails or other policies does the platform maintain to ensure fairness for retail investors in trading against professionals?

4. What controls does the platform maintain to keep unauthorized or abusive traders off the venue?

5. What policies are in place to prevent the company and its employees from exploiting non-public information to benefit themselves at the expense of customers?

6. How does the platform notify customers of a site outage or suspension, the terms under which trading will resume, and how customers can access funds during an outage?

7. What steps does the platform take to subject its security, its virtual and fiat accounts, and its controls to independent auditing or verification?

8. Is the platform subject to, and registered under, state-level banking regulations or a similar oversight regime – for instance, the New York BitLicense regulations?

The report reflects responses from the following platforms: (1) Bitfinex (operated by iFinex Inc.); (2) bitFlyer USA, Inc.; (3) Bitstamp Ltd.; (4) Bittrex, Inc.; (5) Coinbase, Inc.; (6) Gemini Trust Company; (7) HBUS Inc.; (8) itBit (operated by Paxos Trust Company); (9) Poloniex (owned by Circle Internet Financial Limited); and (10) Tidex (operated by Elite Way Developments LLP). Four platforms originally contacted – Binance Limited, Gate.io (operated by Gate Technology Incorporated), Huobi Global Limited, and Kraken (operated by Payward, Inc.) – claimed they did not allow trading from New York and declined to participate. The Attorney General's office investigated those claims and found that Binance, Gate.io, and Kraken all accepted trades from within New York State. As such, the office referred Binance, Gate.io, and Kraken to the New York State Department of Financial Services for potentially operating in New York State without seeking or receiving approval from DFS to engage in a virtual currency business activity.

The report focuses on the practices of the platforms based on the information provided, and takes no position on whether virtual currency itself represents a sound investment decision.

The Virtual Markets Integrity Report was prepared by Senior Advisor and Special Counsel to the Attorney General Simon Brandler; Senior Enforcement Counsel John Castiglione and Assistant Attorney General Brian Whitehurst of the Investor Protection Bureau; and Assistant Attorney General Joseph Mueller of the Consumer Frauds & Protection Bureau; and was overseen by Investor Protection Bureau Chief Cynthia Hanawalt and Chief of Staff Brian Mahanna. The Investor Protection Bureau and Consumer Frauds & Protection Bureau are part of the Economic Justice Division, which is led by Executive Deputy Attorney General Manisha M. Sheth.

The Office of the Attorney General also recognizes the valuable assistance of Marcus Williams and Eric Steinborn of the Administration Division in designing the report.