

# VIRTUAL MARKETS

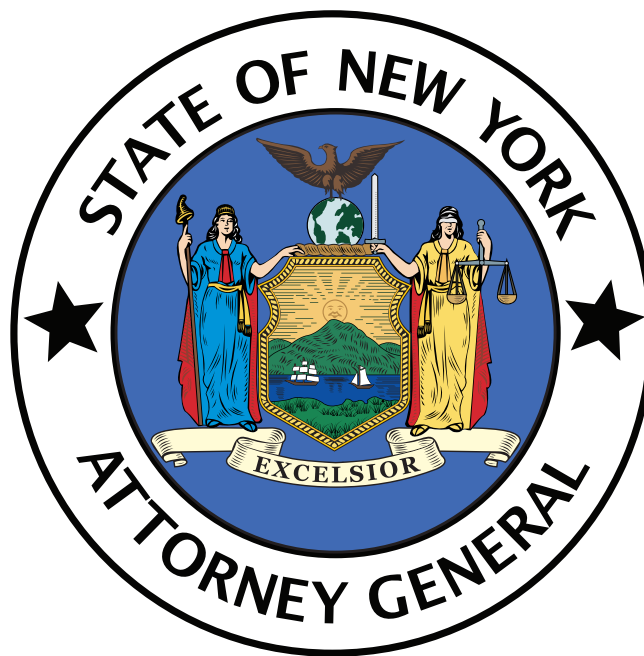
---

# INTEGRITY INITIATIVE

---

## REPORT

---



**Office of the New York State  
Attorney General**

**Barbara D. Underwood  
Attorney General**

September 18, 2018



## INTRODUCTION

The New York State Office of the Attorney General (the “OAG”) launched the Virtual Markets Integrity Initiative to protect and inform New York residents who trade in virtual or “crypto” currency. As a medium of exchange, an investment product, a technology, and an emerging economic sector, virtual currency is complex and evolving rapidly. The OAG’s Initiative, however, proceeds from a fundamental principle: consumers and investors deserve to understand how their financial service providers operate, protect customer funds, and ensure the integrity of transactions.

### VIRTUAL CURRENCY TRADING PLATFORMS

Public interest in virtual currency – bitcoin, ether, and other digital units used to store or exchange value – has increased significantly. The best-known virtual currency, bitcoin, was created less than a decade ago and is now valued at over \$100 billion.<sup>1</sup> Another virtual currency, ether, went from an abstract concept described in a “white paper” to a tradeable asset valued at over \$20 billion in less than five years. There are currently more than 1,800 different virtual currencies exchanged around the world, with more released each month. No longer the exclusive province of tech-savvy hobbyists and traders, virtual currency now appeals to Wall Street firms and “mom-and-pop” retail investors.

To access the virtual currency marketplace, investors rely on virtual asset trading platforms, often referred to as “exchanges.” These online platforms match buyers and sellers of virtual currency, performing functions similar to traditional stock exchanges, private trading venues, and broker-dealers. But unlike those traditional players, virtual asset trading platforms now in operation have not registered under state or federal securities or commodities laws. Nor have they implemented common standards for security, internal controls, market surveillance protocols, disclosures, or other investor and consumer protections.

Accordingly, customers of virtual asset trading platforms face significant risks. In recent years, hackers have infiltrated trading platforms and stolen billions of dollars’ worth of virtual currency, leaving customers with little or no recourse. Delays and outages on trading platforms are common, leaving customers unable to withdraw funds and susceptible to significant losses given volatile prices. Public reports also have linked certain trading platforms to deceptive and predatory practices, market manipulation, and insider abuses.

Trading platforms vary in how they have responded to these risks. Some have taken significant, concrete steps to improve the safety, reliability, and transparency of their operations. Others have not. Meanwhile, customers have had limited access to the information needed to assess the security and fundamental fairness of platforms, or to comparison shop among them.

---

<sup>1</sup> All descriptions of the size and scope of the virtual currency market or the capitalization of any particular currency are current as of September 2018, and are denominated in U.S. dollars.

## THE VIRTUAL MARKETS INTEGRITY INITIATIVE

The OAG enforces laws that protect investors and consumers from unfair and deceptive practices and that safeguard the fairness and integrity of the financial markets. To that end, in April 2018, the OAG commenced the Virtual Markets Integrity Initiative (the “Initiative”), a fact-finding inquiry into the policies and practices of virtual asset trading platforms. The OAG sent letters and questionnaires to thirteen major trading platforms. A sample letter follows this Report as [Appendix A](#). The questionnaire ([Appendix B](#)) sought details on the platforms’ trading operations, as well as information about how the platforms protect customer assets. The OAG’s questions also reflected areas of special concern for everyday retail customers, such as site outages, fees, and the effects of automated or “bot” trading.

The OAG sought voluntary participation, expecting that platforms would embrace the opportunity to provide the public with much-needed clarity regarding basic practices and functionality. Most did. Nine of the thirteen platforms participated in the Initiative: Bitfinex (operated by iFinex Inc.), bitFlyer USA, Inc., Bitstamp, Ltd.,<sup>2</sup> Bittrex, Inc., Coinbase, Inc., Gemini Trust Company, itBit (operated by Paxos Trust Company), Poloniex (owned by Circle Internet Financial Limited), and Tidex (operated by Elite Way Developments LLP). The OAG separately invited HBUS – a platform that calls itself the U.S. “strategic partner” of Huobi Inc. – to respond, as the platform opened for trading in July 2018. HBUS elected to do so, and its responses are included in this Report. The information provided by these platforms forms the basis of this Report. Four platforms – Binance Limited, Gate.io (operated by Gate Technology Incorporated), Huobi Global Limited, and Kraken (operated by Payward, Inc.) – claimed they do not allow trading from New York and declined to participate. The OAG investigated whether those platforms accepted trades from within New York State. Based on this investigation, the OAG referred Binance, Gate.io, and Kraken to the Department of Financial Services for potential violation of New York’s virtual currency regulations.

After compiling and analyzing responses, and comparing them to the platforms’ public disclosures, the OAG gave platforms the opportunity to confirm the information they provided. Nine did.<sup>3</sup>

---

<sup>2</sup> Bitstamp, Ltd. incorporated a Delaware-based entity, Bitstamp USA, Inc., for the U.S. market, which is expected to be operational in the future. Bitstamp, Ltd. is the entity currently accepting transactions from U.S. customers.

<sup>3</sup> Tidex posted partial responses to the questionnaire online and did not provide the OAG with contact information to permit follow-up on the information set forth therein. Nor did Tidex respond to repeated later requests for confirmation submitted to publicly identified email addresses.

## THE VIRTUAL MARKETS INTEGRITY REPORT

The Virtual Markets Integrity Report (the “Report”) addresses areas of particular concern to the transparency, fairness, and security of virtual asset trading platforms, and highlights key policies and practices of the responding platforms. The Report includes the following sections:

**SECTION I: JURISDICTION, ACCEPTANCE OF CURRENCIES, AND FEES.** This section discusses how customers sign up with trading platforms, the access controls in place at the platforms, their acceptance of fiat currency (*i.e.*, traditional, government-issued currency), and their fee structures.

**SECTION II: TRADING POLICIES AND MARKET FAIRNESS.** This section addresses the trading rules in place at the trading platforms and the fairness for retail investors, and includes discussion of order types, the availability of credit (margin trading), policies on automated or algorithmic trading, and measures taken (if any) to address market manipulation and other abusive trading practices.

**SECTION III: MANAGING CONFLICTS OF INTEREST.** This section addresses potential conflicts that may arise between the interests of virtual asset trading platforms, their employees, and their customers.

**SECTION IV: SECURITY, INSURANCE, AND PROTECTING CONSUMER FUNDS.** This section covers the use of independent auditing by the trading platforms, their independent security testing, and their safeguarding of customer funds through insurance and other means.

**SECTION V: ACCESS TO CUSTOMER FUNDS, SUSPENSIONS, AND OUTAGES.** This section discusses select issues concerning customer transactions and withdrawals, policies for suspending trading activity, including customer notification in the event of outages or scheduled maintenance.

Each section presents the responses of participating platforms to specific, targeted questions on topics relevant to retail customers. Examples include:

- (1) Does the platform conduct independent testing to ensure adequate IT security against threats, including hackers?
- (2) Does the platform allow professional traders to use automated or algorithmic trading?
- (3) Does the platform trade against its own customers on its venue?
- (4) Does the platform carry insurance that would cover virtual currency losses in the event of theft or hacking?
- (5) Does the platform compile, disclose, and explain site outages or trading suspensions?

## LIMITATIONS OF THIS REPORT

This Report does not address whether virtual currency represents a sound investment decision. Unlike traditional stocks and commodities, virtual currency is neither tied to a tangible asset nor to the performance of a particular company. The primary driver of a virtual currency's value appears instead to be the willingness of people to use or trade it. This has led some observers to question whether virtual currency has any underlying value at all, and to liken the intense interest in virtual currency to past speculative investment bubbles. The OAG's Report does not evaluate that issue; rather, the objective of this Report is to provide information on virtual asset trading platforms to customers who have used, or are considering using, those platforms to transact in virtual currency.

This Report reflects the information voluntarily provided by platforms. Although platforms were asked to confirm the information they provided, the OAG cannot assure the accuracy of their responses. Further, while the OAG endeavored to include trading platforms that are widely used in New York, the United States, and abroad, in order to provide a snapshot of the industry, their policies and procedures are not necessarily representative of all trading platforms. Seven of the ten participating platforms—(i) bitFlyer USA; (ii) Bitstamp; (iii) Bittrex; (iv) Coinbase; (v) Gemini; (vi) itBit; and (vii) Poloniex (Circle)—sought approval, directly or through a subsidiary, from the New York State Department of Financial Services (“DFS”) to operate a virtual currency business in New York. Pursuant to DFS requirements, licensed virtual currency firms must maintain policies and practices designed to, among other things, protect deposited funds, prevent money laundering and illegal activity, and respond to other risks. Given those requirements, and ongoing supervision and monitoring by DFS, the customer protections in place at platforms subject to the BitLicense regime are likely to be better than those prevailing at other platforms.

Finally, the virtual asset industry is rapidly evolving. Trading platforms are constantly refining and changing their operations, and may elect to reform policies based on market conditions, regulatory requirements, or the findings of government agencies, including those contained in this Report. Since the OAG began its Initiative, certain platforms have revised or improved various policies of interest. The information in the Report is current as of September 2018.

## KEY FINDINGS ON THE STATE OF THE VIRTUAL MARKETS

The Initiative revealed that virtual asset trading platforms vary significantly in their comprehensiveness in responding 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. THE VARIOUS BUSINESS LINES AND OPERATIONAL ROLES OF TRADING PLATFORMS CREATE POTENTIAL CONFLICTS OF INTEREST.** Virtual asset trading platforms often engage in several lines of business that would be restricted or carefully monitored in a traditional trading environment. Platforms often serve (i) as venues of exchange, operating the platform on which buyers and sellers trade virtual and fiat currencies; (ii) in a role akin to a traditional broker-dealer, representing traders and executing trades on their behalf; (iii) as money-transmitters, transferring virtual and fiat currency and converting it from one form to another; (iv) as proprietary traders, buying and selling virtual currency for their own accounts, often on their own platforms; (v) as owners of large virtual currency holdings; and, in some cases, (vi) as issuers of a virtual currency listed on their own and other platforms, with a direct stake in its performance. Additionally, platform employees – who may have access to information about customer orders, new currency listings, and other non-public information – often hold virtual currency and trade on their own or competing platforms. Each role has a markedly different set of incentives, introducing substantial potential for conflicts between the interests of the platform, platform insiders, and platform customers.
- 2. TRADING PLATFORMS HAVE YET TO IMPLEMENT SERIOUS EFFORTS TO IMPEDE ABUSIVE TRADING ACTIVITY.** Though some virtual currency platforms have taken steps to police the fairness of their platforms and safeguard the integrity of their exchange, others have not. Platforms lack robust real-time and historical market surveillance capabilities, like those found in traditional trading venues, to identify and stop suspicious trading patterns. There is no mechanism for analyzing suspicious trading strategies across multiple platforms. Few platforms seriously restrict or even monitor the operation of “bots” or automated algorithmic trading on their venues. Indeed, certain trading platforms deny any responsibility for stopping traders from artificially affecting prices. Those factors, coupled with the concentration of virtual currency in the hands of a relatively small number of major traders, leave the platforms highly susceptible to abuse. Only a small number of platforms have taken meaningful steps to lessen those risks.
- 3. PROTECTIONS FOR CUSTOMER FUNDS ARE OFTEN LIMITED OR ILLUSORY.** 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 whether platforms are responsibly holding their customers’ virtual assets as claimed. Customers are highly exposed in the event of a hack or unauthorized withdrawal. While domestic or foreign deposit insurance may compensate customers

for certain losses of stolen or misappropriated fiat currency, no similar compensation is available for virtual currency losses. There are serious questions about the scope and sufficiency of the commercial insurance that certain platforms purport to carry to cover virtual asset losses. Other platforms do not insure against virtual asset losses at all.

\* \* \*

By highlighting these weaknesses, as well as other considerations important to consumers, the OAG hopes to educate customers, and to encourage the virtual asset marketplace to adopt policies that ensure the integrity of transactions. As the sector matures, the OAG expects responsible trading platforms – in coordination with consumer advocates, regulators, and law enforcement – to expand the transparency, security, fairness, and accountability of their businesses.



## I. JURISDICTION, ACCEPTANCE OF CURRENCIES, AND FEES

It is difficult for ordinary customers to find and compare certain basic – but important – features of virtual asset trading platforms. In order to assist customers in making educated choices, the OAG requested certain basic information from participating platforms, including:

- Where, geographically, a platform is incorporated and headquartered;
- The jurisdictions from which customers are authorized to trade;
- Measures taken to limit access to authorized customers;
- Acceptance of traditional fiat currency, such as Euros and U.S. dollars; and
- Fees associated with maintaining an account and trading.

These basic topics are important for customers to understand. *First*, while several virtual asset trading platforms are located or otherwise licensed to operate in New York, or elsewhere in the United States, others are located in the United Kingdom, Taiwan, or other offshore jurisdictions like the Cayman Islands. In the past, some platforms have moved their operations with little or no warning. For legal and other reasons, many platforms purport not to accept customers from particular geographic locations; indeed, certain platforms claim not to accept customers from anywhere in the United States, or from particular U.S. states.

*Second*, each platform chooses for itself which virtual currencies to list for trading. Certain trading platforms allow customers to deposit U.S. dollars, Euros, or other fiat currency and convert that money into virtual currency. Platforms without banking relationships only facilitate transactions exclusively involving virtual assets. Some platforms limit trading to a few, better-known virtual currencies such as bitcoin or ether; others facilitate the trading of dozens or even hundreds of different virtual currencies, sometimes including virtual currencies they issue themselves.<sup>4</sup>











*Third*, virtual asset trading platforms differ in how they assess fees on customers. As a general matter, trading platforms charge customers on a per-transaction basis, with the amount charged related to the amount of virtual or fiat currency exchanged in a given transaction. Importantly, though, the platforms reported an array of approaches for assessing fees, to whom, and in what amount. Platforms also typically assess deposit and withdrawal fees when customers transfer fiat currency into and out of their accounts.

---

<sup>4</sup> For instance, the Gemini platform allows customers to trade in bitcoin, ether, and Zcash; the trading venue operated by Coinbase (recently re-branded as “Coinbase Pro”) allows customers to trade in bitcoin, ether, Ethereum Classic, Bitcoin Cash, and Litecoin. The Bittrex platform, on the other hand, allows customers to trade dozens of virtual currencies, with names like “ZenCash,” “Storj,” “Lunyr,” “BitCrystals,” and others.

## A. JURISDICTIONS AND AUTHORIZED USE

Given the volatility of the virtual markets, the short track record of trading platforms, and well-publicized problems in the industry, customers should consider where their platform operator is located. The jurisdiction where a platform is incorporated or headquartered may dictate whether and how the customer can seek compensation or other legal recourse in the event his or her data is breached, customer funds are stolen, or a platform becomes insolvent.<sup>5</sup>

JURISDICTION					
					
Incorporation	British Virgin Islands	California	United Kingdom	Delaware	Delaware
Headquarters	Tawain	California	United Kingdom	Washington	California
Prohibited US Jurisdictions	Prohibited in all of the United States	Connecticut, Hawaii, Minnesota, Nevada, West Virginia, & Wyoming	Hawaii & Washington	Available Everywhere	Hawaii
					
Incorporation	New York	Delaware	New York	Delaware	United Kingdom/ Cayman Islands
Headquarters	New York	California	New York	Massachusetts	Unknown
Prohibited US Jurisdictions	Hawaii	Alabama, Arizona, Connecticut, Georgia, Louisiana, New York, North Carolina, Hawaii, Vermont, & Washington	Tennessee & Texas	New York, New Hampshire & Washington	Prohibited in all of the United States

The platforms that refused to respond to OAG’s Initiative – Binance, Gate.io, Huobi, and Kraken – are located in other countries or, in the case of Kraken, headquartered in California. Binance reportedly moved its operations to Malta, after initially locating in Tawain and then Japan. Huobi is reportedly based in Singapore. The location of the operator of Gate.io – which transacts tens of millions of dollars’ worth of virtual currency per day – is unclear from public sources. The company, however, represented in writing to the OAG that the platform is based primarily in China.

Customers must also understand the jurisdictions from which their virtual asset trading platforms purport to prohibit trading, and other restrictions on trading in the platform’s terms of service. Several states, including New York, require companies that run a virtual asset trading platform to obtain approval to operate (and submit to oversight) or to adhere to other rules concerning how they administer their platforms. Moreover, a platform may elect to establish additional trading restrictions in its terms of service. Customers may find ways to circumvent

<sup>5</sup> Bank of England Prudential Conduct Authority, “Dear CEO Letter: Existing or Planned Exposure to Crypto-assets,” (June 28, 2018), available at <https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/letter/2018/existing-or-planned-exposure-to-crypto-assets.pdf?la=en&hash=21DA12EE4697E4BDF0D6D4E9BFF0DDBEE07FFD36> (“Crypto-assets also raise concerns related to misconduct and market integrity – many appear vulnerable to fraud and manipulation, as well as money-laundering and terrorist financing risks.”).

the restrictions that a platform uses to block such trading. Such customers, however, could find themselves without recourse in the event of a dispute with the platform, or loss of funds due to fraud, theft, or insolvency.

## B. VERIFYING AND MONITORING AUTHORIZED ACCESS

Most virtual asset trading platforms purport to allow only customers from authorized jurisdictions to access their venues, and to exclude customers who violate their policies, including those related to market manipulation and money laundering. Trading platforms without an effective system for verifying and monitoring the identity and location of customers cannot block unauthorized access or ensure the fairness and integrity of their marketplace. Customers should be wary of platforms that allow new customers to on-board without adequate safeguards.<sup>6</sup>











Platforms that have implemented a Know Your Customer (“KYC”) program will engage in various measures to confirm a new customer’s identity before permitting certain types of trading. The OAG nonetheless found that virtual asset trading platforms differ significantly in how they confirm identity and enforce their site access policies. Most participating platforms require customers to submit a range of personal identifying information and government-issued identification before allowing new customers to trade. Bitfinex and Tidex do not, requiring little more than an email address to begin trading virtual currencies. The graphic below reflects the requirements for all customers; platforms may elect to require additional on-boarding information from certain customers based on their risk profile and other factors.


ON-BOARDING				
<b>BITFINEX</b> <ul style="list-style-type: none"> <li>• <b>Virtual-to-Virtual Exchanges</b> <ul style="list-style-type: none"> <li>• Email Address</li> <li>• State/Country of Residence</li> </ul> </li> <li>• <b>Fiat-to-Virtual Exchanges</b> <ul style="list-style-type: none"> <li>• Name</li> <li>• Address</li> <li>• Proof of Address</li> <li>• Email</li> <li>• State/Country of Residence</li> <li>• Mobile Number</li> <li>• Age</li> <li>• Government Issued ID</li> <li>• Banking Information</li> </ul> </li> </ul>	<b>bitFlyer</b> <ul style="list-style-type: none"> <li>• <b>All Transactions</b> <ul style="list-style-type: none"> <li>• Name</li> <li>• DOB</li> <li>• Address</li> <li>• Phone Number</li> <li>• Email</li> <li>• Government-issued photo ID</li> <li>• SSN</li> <li>• Proof-of-Residence</li> </ul> </li> </ul>	<b>Bitstamp</b> <ul style="list-style-type: none"> <li>• <b>All Transactions</b> <ul style="list-style-type: none"> <li>• Name</li> <li>• Address</li> <li>• Proof of Address</li> <li>• Email</li> <li>• Mobile Number</li> <li>• DOB</li> <li>• Nationality</li> <li>• Purpose for Trading</li> <li>• Government Issued ID</li> </ul> </li> <li>• <b>Additional for Fiat Deposit</b> <ul style="list-style-type: none"> <li>• Banking Information</li> </ul> </li> </ul>	<b>BITTREX</b> <ul style="list-style-type: none"> <li>• <b>All Transactions</b> <ul style="list-style-type: none"> <li>• Name</li> <li>• Address</li> <li>• Proof of Address</li> <li>• State/Country of Residence</li> <li>• Email</li> <li>• Mobile Number</li> <li>• DOB</li> <li>• SSN</li> <li>• Government Issued ID</li> <li>• Photo of Your Face</li> </ul> </li> <li>• <b>Additional for Fiat Deposit</b> <ul style="list-style-type: none"> <li>• Banking Information</li> </ul> </li> </ul>	<b>coinbase</b> <ul style="list-style-type: none"> <li>• <b>All Transactions</b> <ul style="list-style-type: none"> <li>• Name</li> <li>• Address</li> <li>• State/Country of Residence</li> <li>• Email</li> <li>• Mobile Number</li> <li>• Age</li> <li>• DOB</li> <li>• Last 4 SSN</li> <li>• Purpose for Trading</li> <li>• Government Issued ID</li> <li>• Source of Funds</li> <li>• Occupation</li> <li>• Employment Information</li> </ul> </li> <li>• <b>Additional for Fiat Deposit</b> <ul style="list-style-type: none"> <li>• Banking Information</li> </ul> </li> </ul>
<b>GEMINI</b> <ul style="list-style-type: none"> <li>• <b>All Transactions</b> <ul style="list-style-type: none"> <li>• Name</li> <li>• Address</li> <li>• Email</li> <li>• Mobile Number</li> <li>• DOB</li> <li>• SSN</li> <li>• Government Issued ID</li> </ul> </li> <li>• <b>Additional for Fiat Deposit</b> <ul style="list-style-type: none"> <li>• Banking Information</li> </ul> </li> </ul>	<b>HBUS</b> <ul style="list-style-type: none"> <li>• <b>Virtual-to-Virtual Exchanges</b> <ul style="list-style-type: none"> <li>• Name</li> <li>• Address</li> <li>• Email</li> </ul> </li> <li>• <b>To Withdraw Virtual Currency</b> <ul style="list-style-type: none"> <li>• Government Issued ID</li> <li>• Picture of Face</li> </ul> </li> </ul>	<b>itBit</b> <ul style="list-style-type: none"> <li>• <b>All Transactions</b> <ul style="list-style-type: none"> <li>• Name</li> <li>• Address</li> <li>• Email</li> <li>• Mobile Number</li> <li>• DOB</li> <li>• SSN</li> <li>• Government Issued ID</li> </ul> </li> <li>• <b>Additional for Fiat Deposit</b> <ul style="list-style-type: none"> <li>• Banking Information</li> </ul> </li> </ul>	<b>POLONIEX</b> <ul style="list-style-type: none"> <li>• <b>All Transactions</b> <ul style="list-style-type: none"> <li>• Name</li> <li>• Address</li> <li>• State/Country of Residence</li> <li>• Email</li> <li>• Mobile Number</li> <li>• SSN</li> <li>• Government Issued ID</li> </ul> </li> </ul>	<b>TIDEX</b> <ul style="list-style-type: none"> <li>• <b>All Transactions</b> <ul style="list-style-type: none"> <li>• Name</li> <li>• Email</li> <li>• Mobile Number</li> </ul> </li> </ul>

<sup>6</sup> “On-boarding” is the process of creating and verifying an account to execute trades on a platform.

Online businesses commonly employ several other methods to control access. One common security measure is to monitor IP addresses. An IP address acts as a unique identifier assigned to a computer connected to the Internet, allowing a website operator to monitor the computers that connect to its site. Among other uses, monitoring IP addresses allows a website operator to determine the approximate geographic location of users and track suspicious behavior coming from a particular computer connection. To evade such monitoring, users can attempt to mask their IP addresses using a virtual private network (“VPN”).<sup>7</sup> By routing computer activity through a third-party network, VPNs can obfuscate the location of a log-in. For IP monitoring to be effective, then, platforms must take reasonable steps to unmask or block customers that attempt to access their site via known VPN connections. While most participating platforms reported that they monitor access by IP address, only Bitstamp and Poloniex (Circle) purported to limit VPN access. That raises questions about the ability of the other trading platforms to restrict access to authorized users only.

**MEASURES FOR LIMITING UNAUTHORIZED ACCESS TO THE PLATFORM**

Trading Platforms	Tracking Computer IP Addresses	Blocking Masked VPN IP Addresses
	<b>YES</b>	<b>NO</b>
	<b>YES</b>	<b>NO</b>
	<b>YES</b>	<b>YES</b>
	<b>YES</b>	<b>NO</b>
	<b>YES</b>	<b>NO</b>
	<b>YES</b>	<b>NO</b>
	<b>YES</b>	<b>NO</b>
	<b>YES</b>	<b>NO</b>
	<b>YES</b>	<b>YES</b>
	<b>YES</b>	<b>NO</b>























### C. ACCEPTANCE OF FIAT CURRENCY

To obtain virtual currency initially, retail customers must typically find a virtual asset trading platform that accepts fiat currency. Not all do. Most trading platforms lack a relationship with a bank and allow only trades involving two virtual currencies (e.g. purchasing bitcoin with ether). To trade on those platforms, customers must first obtain virtual currency elsewhere and transfer it onto the platform. In addition to the convenience associated with accepting fiat currency, traditional banks in the United States and overseas are subject to substantial oversight,

<sup>7</sup> VPNs have many useful and legitimate applications, including as a way to offer increased security when accessing the Internet via a public Wi-Fi network (for instance, in an airport or café).

monitoring, and insurance. The existence of a formal banking relationship therefore offers customers with a useful indicator for evaluating the platform as a business concern. As reflected on the chart below, seven participating platforms accept fiat currency.

FIAT CURRENCY ACCEPTANCE	
ACCEPTS FIAT CURRENCY	ONLY ACCEPTS VIRTUAL CURRENCY
<b>BITFINEX</b>     	 <b>HBUS</b>
 bitFlyer 	<b>POLONIEX</b>
<b>Bitstamp</b>  	<b>TIDEX</b>
 BITTREX 	
<b>coinbase</b>   	
 GEMINI 	
<b>itBit</b>  	



#### D. FEES AND FEE DISCLOSURE

In any trading environment, fees are an important consideration for customers and directly affect trading performance. High or unexpected fees can turn profits into losses. Customers should understand what actions will trigger fees, the size of those fees, and whether any “hidden” or non-obvious charges may be associated with trading activity.<sup>8</sup> Fee transparency is especially important in a complex electronic trading environment like virtual currency, where different fees can apply based on the price of the asset bought or sold, the volume of trades executed by the customer, the order type chosen, or the timing of an order submission. Fee structures may also advantage certain types of traders.

Five participating platforms – bitFlyer USA, Bitstamp, Bittrex, HBUS, and Tidex – purport to charge the same trading fees to all customers with the same trading volume. Bitfinex, Coinbase, itBit, and Poloniex (Circle) employ a so-called “maker-taker” fee model.<sup>9</sup> Gemini employs a hybrid fee structure, offering the same trading fees for low-volume customers, but

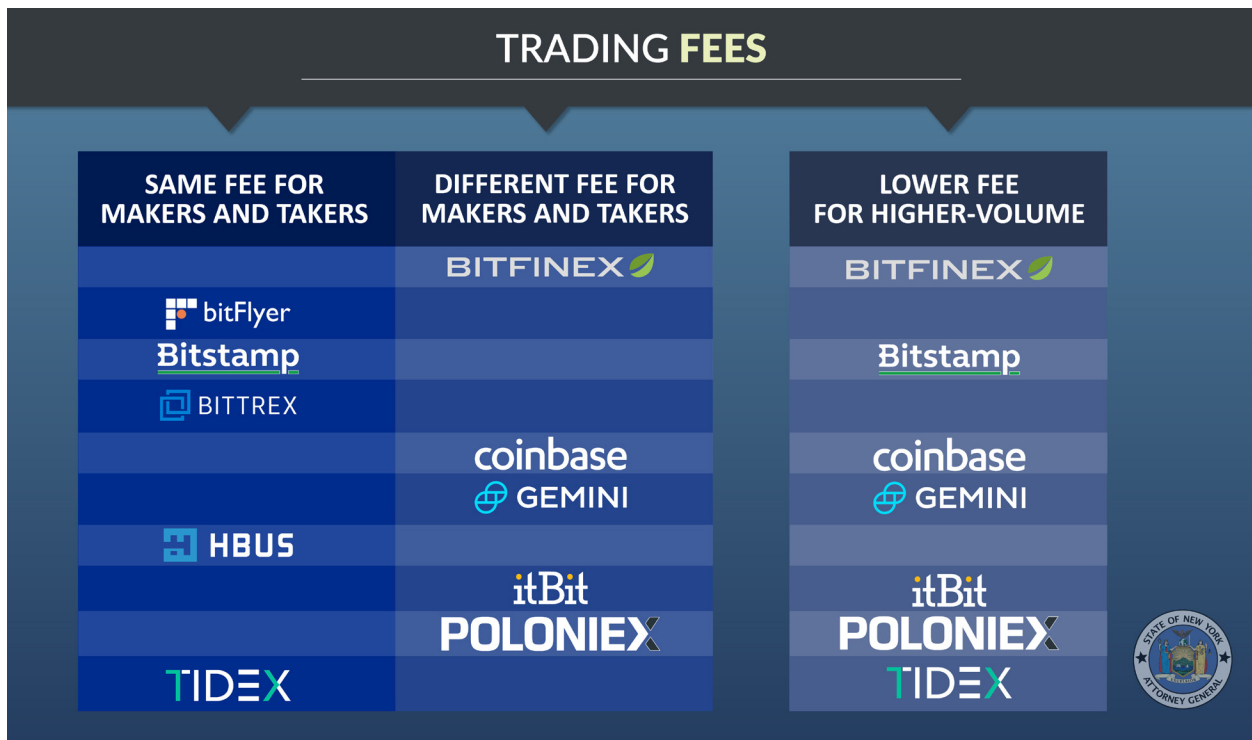
<sup>8</sup> This fundamental principle applies to every financial transaction and asset purchase. OAG Report on Mutual Fund Fees and Active Share, April 2018, available at [https://ag.ny.gov/sites/default/files/ny\\_ag\\_report\\_on\\_mutual\\_fund\\_fees\\_and\\_active\\_share.pdf](https://ag.ny.gov/sites/default/files/ny_ag_report_on_mutual_fund_fees_and_active_share.pdf) (finding that “individual investors do not have access to certain information that would allow them to assess whether the fees they are paying are acceptable” given the services being offered by certain actively managed mutual funds).

<sup>9</sup> See Securities and Exchange Commission Market Structure Advisory Committee Memorandum, “Maker-Taker Fees on Equities Exchanges,” October 20, 2015, available at <https://www.sec.gov/spotlight/emsac/memo-maker-taker-fees-on-equities-exchanges.pdf> (describing, among other things, the historical development of “maker-taker” pricing in the equities markets).

applying maker-taker pricing to high-volume traders. Although HBUS’s fee schedule lists separate fees for makers and takers, it currently charges the same rates to both.

“Maker-taker” is a fee model that charges lower or no fees to customers who “make” liquidity (i.e., whose orders exist on the order book prior to a trade), whereas customers who “take” liquidity by filling an already-existing order are charged more.

As discussed in further detail in Section II, “maker-taker” fee models favor professional traders over retail customers, and may create incentives that distort the market.



Importantly, while Bittrex is the only participating platform not to offer volume discounts to high-volume customers, bitFlyer USA, Bitstamp, Gemini, HBUS, and itBit disclosed to the OAG that certain traders may receive different, and presumably preferential, pricing according to the terms of confidential bilateral agreements, the details of which are not disclosed in public fee schedules.

Virtual asset trading platforms also charge other fees, including deposit and withdrawal fees for fiat or virtual currency, and other services. Customers should review and understand the complete fee schedule provided by a platform before they trade.

DEPOSIT AND WITHDRAWAL FEES							
DEPOSIT FEES				WITHDRAWAL FEES			
Virtual Currency	Wire Transfers	Credit/Debit Card	No Fees	Virtual Currency	Wire Transfers	Credit/Debit Card	No Fees
BITFINEX	BITFINEX			BITFINEX	BITFINEX		
			bitFlyer	bitFlyer	bitFlyer		
Bitstamp	Bitstamp	Bitstamp			Bitstamp	Bitstamp	
			BITTREX				BITTREX
	coinbase				coinbase		
			HBUS				HBUS
	itBit				itBit		
			GEMINI				GEMINI
			POLONIEX	POLONIEX	POLONIEX		
			TIDEX	TIDEX			

This does not include any transaction/mining fees charged by an individual cryptocurrency

By raising the costs of moving funds onto, and off of, individual platforms, those fees may serve as a disincentive for customers to switch platforms (or exit virtual assets entirely) in response to shifting market conditions. Certain platforms, notably Bittrex and Gemini, purport to charge no withdrawal or deposit fees for most customers.<sup>10</sup>

Customers should understand that the four trading platforms that refused to participate in the OAG’s Initiative may not make their full schedule of fees available publicly, and that certain customers may receive preferential rates. Further, customers should be aware that those venues may not disclose certain fees in advance, and customers could find that transacting on those venues is more expensive than anticipated.

<sup>10</sup> Certain “network transfer fees” may apply, which are fees that are built into the programming of certain virtual currencies.

## II. TRADING POLICIES AND MARKET FAIRNESS

Virtual asset trading platforms have positioned themselves as comparable to traditional stock trading venues. But trading on virtual currency platforms differs in fundamental ways from trading on a regulated stock trading venues. Customers should be aware of the differences.<sup>11</sup>

Understanding the general structure of the traditional securities marketplace is helpful for understanding how virtual asset trading platforms are different, and why that matters to customers. The traditional “public” stock exchanges (e.g., the New York Stock Exchange or Nasdaq) must submit information regarding virtually all important aspects of their operations to the Securities and Exchange Commission (“SEC”) for review prior to implementation.<sup>12</sup> Similarly, alternative trading systems (“ATS”) – of which there are several dozen in the United States – are private stock trading venues operated by a broker-dealer. ATSs are subject to extensive disclosure obligations regarding their ownership, operation, and rules. Those disclosures are designed to allow traders to understand the material aspects of how the ATSs operate.<sup>13</sup> As an additional safeguard, everyday investors access traditional stock trading venues through a registered broker-dealer (or via personal investment advisor) whose business it is to understand the often-complicated nature of trading in order to effectively act on behalf of their clients.<sup>14</sup>

In contrast, virtual asset trading platforms are not currently registered as trading venues under federal securities laws. Further, customers access virtual asset trading platforms directly, submitting orders themselves. Trading platforms claim that the ability to freely access their venues benefits customers. This freedom, however, requires everyday customers to understand not only how each trading platform operates as a venue of exchange (and to understand the differences among platforms), but also to make judgments about how to monitor quickly-moving prices, select appropriate order types, place trades, and accurately monitor performance, without guidance from a professional with knowledge and experience.

---

<sup>11</sup> Securities and Exchange Commission, “Statement on Potentially Unlawful Online Platforms for Trading Digital Assets,” (Mar. 7, 2018), available at <https://www.sec.gov/news/public-statement/enforcement-tm-statement-potentially-unlawful-online-platforms-trading> (“The SEC staff has concerns that many online trading platforms appear to investors as SEC-registered and regulated marketplaces when they are not. Many platforms refer to themselves as ‘exchanges,’ which can give the misimpression to investors that they are regulated or meet the regulatory standards of a national securities exchange.”).

<sup>12</sup> Securities and Exchange Commission, “The Laws That Govern the Securities Industry,” available at <https://www.sec.gov/answers/about-lawsshtml.html#secexact1934> (“The exchanges . . . are identified as self-regulatory organizations (SRO). SROs must create rules that allow for disciplining members for improper conduct and for establishing measures to ensure market integrity and investor protection. SRO proposed rules are subject to SEC review and published to solicit public comment. While many SRO proposed rules are effective upon filing, some are subject to SEC approval before they can go into effect.”).

<sup>13</sup> Securities and Exchange Commission, “Alternative Trading System (‘ATS’) List,” available at <https://www.sec.gov/foia/docs/atstlist.htm> (“An ATS is a trading system that meets the definition of ‘exchange’ under federal securities laws but is not required to register as a national securities exchange . . . To comply with Regulation ATS, an ATS must, among other things, register as a broker-dealer and file an initial operation report with the Commission on Form ATS before commencing operations. Thereafter, an ATS must file amendments to Form ATS to provide notice of any changes to its operations.”). Recently, the SEC adopted new rules to enhance the transparency and oversight of ATSs. Securities and Exchange Commission, “SEC Adopts Rules to Enhance Transparency and Oversight of Alternative Trading Systems,” (July 18, 2018), available at <https://www.sec.gov/news/press-release/2018-136>.

<sup>14</sup> For a thorough description of the laws and rules governing the activities of broker-dealers and other related topics, see New York State Office of the Attorney General, “Brokers, Dealers, Salespersons,” available at <https://ag.ny.gov/investor-protection/brokers-dealers-salespersons>; see also Securities and Exchange Commission, “Guide to Broker-Dealer Registration,” (April 2008), available at <https://www.sec.gov/reportspubs/investor-publications/divisionsmarketregbdguidehtm.html>.



Several prominent virtual asset trading platforms have also developed products and services that appeal to, and advantage, sophisticated professional electronic traders, increasing risks for retail traders. For instance, some platforms offer high-speed direct market data feeds to professional traders, and permit traders to “co-locate” or “cross-connect” their trading computers to the platform’s servers, accessible through electronic “FIX protocol” messaging systems.<sup>15</sup> Platforms also offer the previously discussed “maker-taker” pricing models. Those products and services are designed to allow professional traders to leverage data and speed to power sophisticated automated trading strategies – strategies that can negatively affect the trading performance of everyday, non-automated customers.<sup>16</sup>

To assist customers in understanding these issues, the OAG asked trading platforms to provide information on several key topics:

- Special features provided to professional traders, including specialized order types, direct data feeds, co-location, “maker-taker” pricing, etc.;
- Policies, if any, regarding platform access by automated trading algorithms;
- Policies regarding potential abusive trading practices; and
- Margin trading.

#### **A. SPECIAL FEATURES TO PREFERENCE PROFESSIONAL TRADERS**

The modern electronic stock trading environment is replete with features that provide professional traders with an extremely fast, data-rich view of the markets, and the means with which to accomplish their specialized strategies. Sophisticated traders also take advantage of the fee structures of many stock trading venues, some of which were discussed above, that are designed to encourage certain types of sophisticated, professional trading activity.<sup>17</sup>

Complex order types are another way professional traders may have a comparative advantage over other platform customers. Like trading other asset classes, trading virtual currency is more complicated than just choosing to “buy” or “sell.” Trading platforms offer a variety of different order types, allowing customers who understand how those order types work to tailor their trading strategy. Choosing the right order type has a significant effect on whether, and at what price, an order will execute.<sup>18</sup> For example, some trading platforms offer order types

<sup>15</sup> “FIX” stands for “Financial Information eXchange.” FIX protocol is an electronic messaging protocol used by the financial services industry, allowing parties to an electronic trade to automatically pass along information about orders and executions.


<sup>16</sup> See Securities and Exchange Commission, Release No. 34-82873 (March 14, 2018), available at <https://www.sec.gov/rules/proposed/2018/34-82873.pdf> (proposing pilot study on transaction fee pricing models; “In recent years, a variety of concerns have been expressed about the maker-taker fee model, in particular the rebates they pay to attract orders. For example, some have questioned whether the prevailing fee structure has created a conflict of interest for broker-dealers, who must pursue the best execution of their customers’ orders while facing potentially conflicting economic incentives to avoid fees or earn rebates—both of which typically are not passed through the broker-dealer to its customers—from the trading centers to which they direct those orders for execution.”).

<sup>17</sup> For more information on automated trading strategies, see FINRA, “Getting Up to Speed on High-Frequency Trading,” (Nov. 25, 2015), available at <http://www.finra.org/investors/getting-speed-high-frequency-trading>.

<sup>18</sup> There are a number of useful and informative resources available describing how different order types work. See, e.g., Securities and Exchange Commission, “Investor Bulletin: Understanding Order Types,” (July 12, 2017), available at [https://www.sec.gov/oia/investor-alerts-and-bulletins/ib\\_ordertypes](https://www.sec.gov/oia/investor-alerts-and-bulletins/ib_ordertypes); Vanguard, “Order Types and How They Work,” available at <https://investor>.

like the so-called “Fill-or-Kill,” in which the order is canceled in its entirety if it does not execute immediately and in full; “Immediate-or-Cancel,” in which all or a part of an order must execute immediately and any remaining unfilled portions of the order are canceled; or “Post-Only,” (also known as “Maker-or-Cancel”), in which the order only posts to the order book if it would not fill an already-posted order. Some platforms, such as Bitfinex, offer an order type called “hidden,” in which the “hidden” order does not appear on the publicly visible order book.

ORDER TYPE				
<b>BITFINEX</b> <ul style="list-style-type: none"> <li>• Market</li> <li>• Limit</li> <li>• Stop</li> <li>• Stop-Limit</li> <li>• Trailing Stop</li> <li>• Fill-or-Kill</li> <li>• Scaled</li> <li>• One Cancels Other</li> <li>• Hidden</li> <li>• Post-Only</li> </ul>	<b>bitFlyer</b> <ul style="list-style-type: none"> <li>• Market</li> <li>• Limit</li> <li>• Stop</li> <li>• Stop-Limit</li> <li>• Trailing Stop</li> <li>• Immediate-or-Cancel</li> <li>• Good Till Cancelled</li> <li>• Fill-or-Kill</li> </ul>	<b>Bitstamp</b> <ul style="list-style-type: none"> <li>• Market</li> <li>• Limit</li> <li>• Instant</li> <li>• Good Till Cancelled</li> <li>• Immediate-or-Cancel</li> <li>• Good Till Date</li> <li>• Good Till End of Day</li> </ul>	<b>BITTREX</b> <ul style="list-style-type: none"> <li>• Market</li> <li>• Limit</li> <li>• Limit-by-Time</li> </ul>	<b>coinbase</b> <ul style="list-style-type: none"> <li>• Market</li> <li>• Limit</li> <li>• Stop Market</li> <li>• Stop Limit</li> <li>• Good Till Cancel</li> <li>• Immediate-or-Cancel</li> <li>• Fill-or-Kill</li> </ul>
<b>GEMINI</b> <ul style="list-style-type: none"> <li>• Market</li> <li>• Limit</li> <li>• Immediate-or-Cancel</li> <li>• Auction Only Limit</li> <li>• Indication of Interest</li> <li>• Maker-or-Cancel</li> </ul>	<b>HBUS</b> <ul style="list-style-type: none"> <li>• Market</li> <li>• Limit</li> </ul>	<b>itBit</b> <ul style="list-style-type: none"> <li>• Limit</li> </ul>	<b>POLONIEX</b> <ul style="list-style-type: none"> <li>• Market</li> <li>• Limit</li> <li>• Stop-Limit</li> </ul>	<b>TIDEX</b> <ul style="list-style-type: none"> <li>• Not Specified</li> </ul>



Offering special order types does not necessarily benefit retail customers given the difficulty of learning and deploying the more complex options. In fact, many order types are only useful to professional, automated traders using sophisticated algorithmic strategies, where orders can be submitted and cancelled automatically, in response to market signals not visible (or even available) to regular traders. To give customers a better sense of the order types available, the OAG asked the trading platforms to describe the order types they offer.

**Customers should be aware that the platforms that refused to participate in the OAG’s Initiative (Binance, Gate.io, Huobi, and Kraken) may not disclose all order types offered to certain traders, some of which could preference those traders at the expense of others, and that the trading performance of other customers on those venues could be negatively affected as a result.**

Another feature that tends to favor sophisticated, high-volume traders is the ability to “co-locate” or “cross-connect” their trading computers directly with the platform’s computers in a data center. This gives sophisticated trading operations a faster view of the platform order book than is available to retail customers.<sup>19</sup> The only participating platform to disclose a co-location option to date

[vanguard.com/investing/online-trading/order-types](http://vanguard.com/investing/online-trading/order-types).

<sup>19</sup> Additionally, several firms are reported to have begun offering data analytics about the virtual currency marketplace, allowing

is Gemini. As the virtual currency sector matures, however, more platforms may make co-location or cross-connection available to professional traders. Alongside so-called “maker-taker” pricing models and volume pricing discounts that create incentives for professional traders to direct their orders to that platform (See Section I, “Fees and Fee Disclosure”), those features can distort the overall trading environment, to the detriment of retail customers.

## **B. POLICIES REGARDING AUTOMATED TRADING**

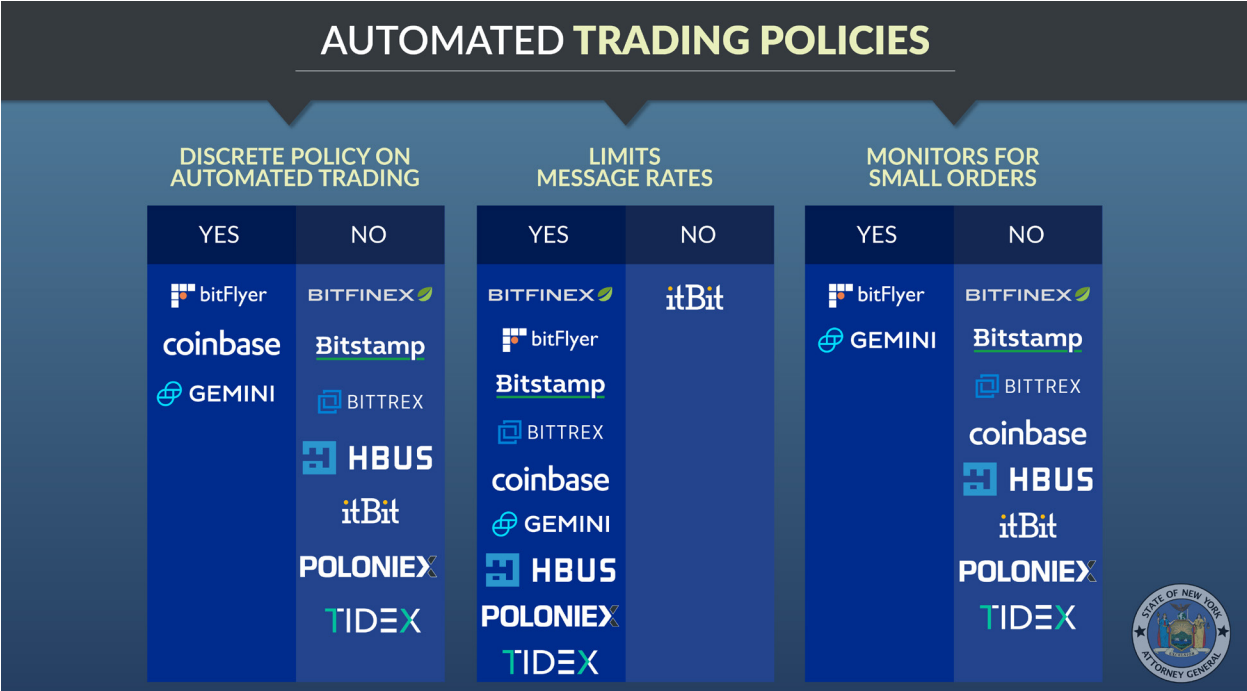
Certain abusive trading practices can be accomplished using computer-automated or “bot” trading strategies. For example, the submission of multiple, illusory orders to a trading platform could be used to artificially move the price of a particular asset, or to negatively impact the speed or responsiveness of the platform. Automated trading activities could also allow a single trader or group of traders to command multiple accounts simultaneously to obscure coordinated trading, in order to manipulate prices.

To better understand these sorts of risks, the OAG asked platforms whether automated trading is permitted, and what – if any – policies or procedures are in place concerning automated trading strategies. Participating platforms uniformly reported that they permit automated trading. Most reported to the OAG that their platform can be accessed via an application programming interface (an “API”), which allows traders to automatically send and receive trading information, and which automated trading algorithms use to participate on the platform. Of particular concern, however, several platforms reported that they had no formal policies governing automated trading. Some claimed that automated trading behavior is “monitored,” without providing detail. Other platforms claimed to have implemented strategies to limit “message rates” submitted to the exchange (high message rates are often a marker of an abusive trading strategy), or to suspend or block traders that submitted an excessive number of small orders in a given timeframe (another potential marker of an abusive or fraudulent trading strategy).<sup>20</sup>

---

professional traders even more data-rich sources of information to enhance their ability to trade virtual currencies. See, e.g., Coindesk, “Nasdaq Said to Be Building Tool to Predict Crypto Price Movements,” (Sept. 11, 2018), available at <https://www.coindesk.com/nasdaq-said-to-be-building-tool-to-predict-crypto-price-movements/>; Thomson Reuters, “Thomson Reuters Expands Sentiment Data to Track Top 100 Cryptocurrencies,” (June 13, 2018), available at <https://www.thomsonreuters.com/en/press-releases/2018/june/thomson-reuters-expands-sentiment-data-to-track-top-100-cryptocurrencies.html>; Coindesk, “NYSE Parent Company Launches Cryptocurrency Data Feed,” (Jan. 18, 2018), available at <https://www.coindesk.com/nyse-parent-company-launches-crypto-trading-data-stream-for-exchanges/>.

<sup>20</sup> Certain platforms reported that this sort of “messaging limit” was a feature of their API (programmed to only accept a certain number of incoming messages from a given user over a particular time frame); others reported that they actively monitored for excessive messages from users, which could be a sign of abusive or manipulative trading behavior.



Customers should be aware that the platforms that refused to participate in the OAG’s Initiative may not restrict the access and use of potentially abusive automated trading strategies. This could adversely affect customers’ trading performance, including the prices at which virtual or fiat currency exchanges take place, and it calls into question the fairness of the platform to retail customers.

**C. POLICIES TO PREVENT MARKET MANIPULATION AND ABUSIVE TRADING**






The steps a virtual asset trading platform takes to monitor and stop manipulative or abusive trading activity on the venue matters for its customers and the integrity of the virtual market as a whole. Because the prices of virtual assets move in concert across different venues, manipulative activity on one venue affects prices and liquidity on other venues. When any venue tolerates manipulative or abusive conduct, the integrity of the entire market is at risk. The New York Department of Financial Services has directed virtual currency entities operating in New York to adopt measures to identify and investigate fraud and market manipulation – an important element in ensuring the integrity of trading.<sup>21</sup>

The OAG asked trading platforms to describe what, if any, policies were in place to define, detect, prevent, or penalize suspicious trading activity or market manipulation, and to provide a description of trading behavior that the platform believes constitutes manipulative or abusive activity. While participating platforms expressed their commitment to combatting market manipulation, only a few reported having a formal policy in place, defining the types of conduct the platform believes to be manipulative or abusive, and outlining how such trading behavior is to be detected and penalized.<sup>22</sup>

<sup>21</sup> New York Department of Financial Services, “Guidance on Prevention of Market Manipulation and Other Wrongful Activity,” (Feb. 7, 2018), available at <https://www.dfs.ny.gov/legal/industry/il180207.pdf>.

<sup>22</sup> Platforms uniformly prohibit market manipulation in their standard terms of service; the OAG sought information as to formal policies and procedures employed by the platforms.

## FORMAL MARKET MANIPULATION POLICY

FORMAL POLICY	NO FORMAL POLICY
 BITTREX	BITFINEX 
coinbase	 bitFlyer
 GEMINI	<u>Bitstamp</u>
 HBUS	POLONIEX
	itBit
	TIDEX



Each participating platform maintains a policy prohibiting a single user from opening multiple accounts, a restriction which several platforms claimed helps prevent manipulative conduct (like fraudulent wash sales).<sup>23</sup> However, a prohibition against multiple accounts is only effective if a platform can actually detect customers attempting to open multiple accounts. That requires robust on-boarding procedures, including multiple forms of identification verification, and other countermeasures (several of which are discussed in Section IB, “Verifying and Monitoring Authorized Access”). Where a platform – for example, Bitfinex – neither requires documentation to execute a virtual currency trade nor takes active measures to block access via VPN, there is reason to question the effectiveness of that platform’s efforts to address manipulative or abusive trading activity.

The industry has yet to implement serious market surveillance capacities, akin to those of traditional trading venues, to detect and punish suspicious trading activity. A platform cannot take action to protect customers from market manipulation and other abuses if it is not aware of those practices in the first place. Several platforms also told the OAG that it was impossible to effectively surveil for manipulative activity taking place on more than one platform, and so any one trading platform is necessarily limited in the steps it can take to police abusive activity. Some platforms do appear to be taking steps to improve surveillance. Gemini previously disclosed a partnership with traditional stock exchange Nasdaq to use more sophisticated market surveillance tools. At least one other platform disclosed to the OAG that it was in the process of contracting for a similar service.

<sup>23</sup> Fraudulent “wash sales” occur when a trader (or traders acting in concert) buy and sell the same asset repeatedly, in order to create the false appearance of market activity in order to move prices.

The OAG could not review the practices and procedures of non-participating platforms (Binance, Gate.io, Huobi, and Kraken) concerning manipulative or abusive trading. However, the Kraken platform’s public response is alarming. In announcing the company’s decision not to participate in the Initiative, Kraken declared that market manipulation “doesn’t matter to most crypto traders,” even while admitting that “scams are rampant” in the industry.

#### D. MARGIN TRADING

Margin trading accounts allow customers to borrow funds to trade an asset. Margin trading increases risk, exposing traders to much higher losses when a virtual asset investment declines in value. In traditional markets, margin trading is subject to significant regulation and oversight, meant to ensure that investors understand the heightened risks, and to establish appropriate credit risk procedures and limits.<sup>24</sup>

A trading environment where prices are volatile and subject to sharp, unpredictable declines magnifies the inherent risks of margin trading.<sup>25</sup> Only two participating platforms – Bitfinex and Poloniex (Circle) – currently support margin trading.<sup>26</sup> Customers trading on margin should recognize that the volatility of the virtual currency market can cause outsize losses very quickly. This risk is exacerbated during platform suspensions or outages, during which leveraged positions may be “locked in” for an extended period of time.

---

<sup>24</sup> See Securities and Exchange Commission, “Margin: Borrowing Money to Pay for Stocks,” (Apr. 17, 2009), available at <https://www.sec.gov/reportspubs/investor-publications/investorpubsmarginhtm.html>.

<sup>25</sup> BIS Annual Economic Report 2018, available at <https://www.bis.org/publ/arpdf/ar2018e5.pdf> (“cryptocurrencies’ valuations are extremely volatile”); Financial Conduct Authority, “Dear CEO Letter: Cryptoassets and Financial Crime,” (June 11, 2018), available at <https://www.fca.org.uk/publication/correspondence/dear-ceo-letter-cryptoassets-financial-crime.pdf> (describing the use of virtual assets as “high-risk speculative investments”); Office of the Director of National Intelligence, “Risks and Vulnerabilities of Virtual Currency Cryptocurrency as a Payment Method,” (2017), available at [https://www.dni.gov/files/PE/Documents/9---2017-AEP\\_Risks-and-Vulnerabilities-of-Virtual-Currency.pdf](https://www.dni.gov/files/PE/Documents/9---2017-AEP_Risks-and-Vulnerabilities-of-Virtual-Currency.pdf) (noting volatility of cryptocurrencies as deterrent to adoption as a payment method, and other risks). Further, if a platform itself serves as creditor (i.e., the platform loans the money), the platform itself, as a business, is exposed to risk from price volatility.

<sup>26</sup> Publicly available information indicates that each of the non-participating platforms – Binance, Gate.io, Huobi, and Kraken – supports margin trading.

## MARGIN TRADING

OFFERED	NOT OFFERED
	
	
	
	
	
	
	
	



### III. MANAGING CONFLICTS OF INTEREST

One of the challenges faced by investors trading in traditional securities markets is navigating the complex tangle of relationships and incentives that have arisen in the modern market structure. For several years, the OAG has investigated conflicts of interest in the securities markets, uncovering the systemic failures of large broker-dealers to appropriately manage these conflicts, at the expense of their traditional retail and institutional clients.<sup>27</sup> In non-securities contexts, the OAG has taken action against online businesses who failed to implement appropriate internal procedures governing whether and how employees could access and exploit sensitive user data.<sup>28</sup>

Managing conflicts of interest is a serious and growing issue in the virtual marketplace. A review of publicly available information, as well as information provided by trading platforms,

<sup>27</sup> The OAG Press Release (Mar. 22, 2016), available at <https://ag.ny.gov/press-release/ag-schneiderman-announces-record-42-million-settlement-bank-america-merrill-lynch-over> (announcing \$42 million settlement by Bank of America Merrill Lynch to resolve OAG investigation into falsified electronic trade confirmations for orders routed to high-speed “electronic liquidity providers,” and other fraudulent conduct); OAG Press Release (Feb. 1, 2016), available at <https://ag.ny.gov/press-release/ag-schneiderman-announces-landmark-resolutions-barclays-and-credit-suisse-fraudulent> (announcing combined \$154.3 million dollar settlements by Barclays and Credit Suisse to resolve OAG and SEC investigations into false statements and omissions made in connection with the marketing of their respective dark pools and other high-speed electronic equities trading services); OAG Press Release (Dec. 16, 2016), available at <https://ag.ny.gov/press-release/ag-schneiderman-announces-deutsche-bank-will-pay-37-million-penalty-fraudulent-order> (announcing combined \$37 million settlement by Deutsche Bank to resolve OAG and SEC investigation into false statements and omissions made in connection with the marketing of Deutsche Bank’s electronic equities order routing services).

<sup>28</sup> The OAG Press Release (Oct. 25, 2016), available at <https://ag.ny.gov/press-release/ag-schneiderman-announces-12-million-settlement-draftkings-and-fanduel> (announcing \$12 million settlement by daily fantasy sports companies to resolve investigation into false and deceptive practices, illegal operation in New York).

suggests several areas of concern. *First*, there is little information about why trading platforms list a given virtual currency on their venue, and whether payments to the platform (in cash or virtual currency) drive listings. *Second*, the owners and investors in several trading platforms are themselves large holders of virtual assets traded on their venue, with an attendant interest that the prices of those assets continue to rise. *Third*, trading platform employees are often themselves investors in virtual assets, and trade on their own platform against customers, potentially using non-public information to inform their trades. *Fourth*, apart from individual employee trading, several trading platforms themselves trade on their own venue in a proprietary capacity.

Those practices put the interests of customers in tension with the interests of platforms and their employees. In order to protect themselves, customers should seek out platforms that pay careful attention to these issues and use appropriate means to ensure that all traders on the platform are being treated equally and fairly. At the industry level, appropriate management of conflicts of interest is critical if virtual assets are to be integrated into the commercial and financial markets.

The OAG's Initiative sought information about several important issues that directly concern the fairness and transparency of trading platforms, and potential conflicts of interest, including:

- Standards applied when considering whether to list a virtual assets;
- Compensation received for listing virtual assets;
- Policies and procedures regarding platform employee trading s;
- Proprietary company trading on the venue.

#### **A. STANDARDS AND CONSIDERATION RECEIVED FOR LISTING A VIRTUAL ASSET**

Some platforms limit the number of virtual assets they list – for instance, offering trading only in bitcoin – while other platforms list dozens of virtual assets, offering hundreds of potential pairings to trade.<sup>29</sup> As of today, there are no regulatory or even generally accepted prudential standards for determining whether a particular virtual asset can or should be listed on a trading platform. This is in stark contrast to the public stock exchanges, which publish their listing standards.<sup>30</sup>

Accordingly, the OAG asked platforms to provide information regarding how they evaluated virtual assets for listing on their venue – in other words, what, if any, criteria do platforms use in evaluating whether a given virtual currency will be listed for trading? Across the board, the OAG found that platforms' determinations of whether to list a given virtual asset were largely subjective. No platform articulated a consistent methodology used to determine whether and why

<sup>29</sup> Unlike traditional stock trading venues, where each stock is denominated in, and ultimately exchangeable for, dollars, some virtual asset trading platforms do not offer the ability to trade virtual currencies for fiat currency. Trades are made available in "pairs," meaning that one virtual currency is available to be traded in exchange for another virtual currency – for instance, ether-to-bitcoin, ether-to-litecoin, etc.

<sup>30</sup> See New York Stock Exchange Listed Company Manual, available at <http://wallstreet.cch.com/LCM/Sections/>; Nasdaq Continued Listing Guide, available at <https://listingcenter.nasdaq.com/assets/continuedguide.pdf>; IEX Listing Guide, available at <https://iextrading.com/docs/IEX%20Listing%20Guide.pdf>.



it would list a given virtual asset. Some objective factors did appear to be considered by many. For instance, platforms often look at the total value or “market capitalization” of a virtual asset, or its average daily trading volume. But the OAG found there is no rhyme or reason to how those objective factors are applied, and there is certainly no consistent application across platforms.<sup>31</sup>

Notably, since the announcement of the OAG’s Initiative in April 2018, at least one trading platform – Circle, the operator of Poloniex – publicly announced an “Asset Framework” that sets forth various factors the company will consider when deciding whether to list virtual currency.<sup>32</sup> Transparency like that is helpful. Customers should know what standards a platform uses to evaluate the virtual assets they list, and should have some assurance that assets traded on the venue conform to those standards. Platforms that have not disclosed their listing standards publicly should consider doing so.

Another important issue for consumers is whether a virtual asset trading platform has accepted compensation for listing a virtual currency. Unlike traditional stock exchanges, which publish listing fees, virtual asset trading platforms generally do not disclose the compensation, if any, received for listing a particular virtual currency. This compensation can come in the form of virtual currency, including a share of the new listing, fiat currency, or other inducements. Disclosure of payments or other compensation would allow customers to consider a platform’s incentives in offering or promoting a virtual currency. Accordingly, the OAG asked virtual asset trading platforms to disclose whether they sought or received compensation for listing a virtual currency, and if so, to describe the circumstances.<sup>33</sup> Only one of the participating platforms reported receiving compensation for listing a virtual currency over the last two years: HBUS, which charges a fee tied to the market capitalization of the virtual asset.

**For non-participating platforms (Binance, Gate.io, Huobi, and Kraken), customers should be aware that those platforms may have received compensation for listing virtual currencies on their platform. Customers should evaluate whether that affects their decision to trade virtual currencies on those platforms. One recent report, for example, asserted that Binance had sought millions of dollars in bitcoins in exchange for listing a new token.**

## **B. RESTRICTIONS ON EMPLOYEE TRADING**

Another feature that distinguishes virtual currency trading markets from traditional securities or commodities markets is that the owners and employees of virtual asset trading platforms can trade directly on their own platforms. This stands in contrast to traditional securities markets, where employees do not trade directly on their venue (access to which

<sup>31</sup> In other words, no platform reported having set thresholds that must be reached for an asset to become eligible for listing. For instance, there is no defined level of trading volume or “market capitalization” that has to be reached before an asset becomes eligible to trade.

<sup>32</sup> Circle Asset Framework, available at <https://www.circle.com/marketing/pdfs/en/circle-asset-framework.pdf>.

<sup>33</sup> The OAG sought this information in the context of a broader request for an explanation of revenues received by the trading platforms over the past two years. Accordingly, responses about compensation received for listing were limited to consideration received over the past two years. Certain platforms did report receiving an “administrative fee” to address compliance issues, a practice those platforms stated has since been discontinued.

requires a registered broker-dealer subject to a host of federal or state regulations, as well as the membership requirements of the exchange or subscriber rules of the ATS).<sup>34</sup>

Trading by platform employees poses a conflict of interest. That conflict can be managed if the platform adopts, and its employees adhere to, policies and procedures prohibiting employees from trading on the basis of information that gives them an advantage over customers – for instance, access to non-public news (like the impending listing of a new virtual currency on the platform), information about the status of the platform order book, or information about its customers' identities.

Overall, the OAG's Initiative found a range of different policies at the participating platforms as to whether and how platform owners or employees are permitted to trade on their platform or on other platforms. One platform, HBUS, reported that its employees may not trade on its platform. Other platforms reported to the OAG that while employees could trade on their venue, employees had no informational or other advantage over other traders (for instance, access to non-public order book data). The OAG found that the measures taken to monitor or prevent employee trading differed. Some platforms require employees, or a subset of employees with access to sensitive data (for instance, those with knowledge of forthcoming listings), to be pre-cleared before transacting, while others limited employees' ability to trade on outside platforms, because the platform's ability to monitor activity on a third-party platform is difficult or impossible. Two trading platforms – Gemini and Bittrex – require regular disclosures from each employee concerning their trading history and current virtual asset holdings. Bittrex goes further, by restricting employee trading to a two-day window each quarter. Bitfinex, itBit, and Tidex did not provide any restrictions on employee trading.<sup>35</sup>

**Customers should be aware the platforms that refused to participate in the OAG's Initiative might not limit the access of employees or other insiders to non-public or otherwise sensitive information, or monitor employees trading to ensure that other customers are not being placed at a disadvantage.**

### C. PROPRIETARY TRADING BY PLATFORM OPERATORS

In addition to permitting employees to trade for their own personal accounts, several platforms reported that they engage in proprietary trading on their own venue. In other words, customers who submit an order to buy or sell a virtual asset could have their order filled not by another customer, but by a "trading desk" run by the platform itself, trading on behalf of the platform for its own account.











There are reasons why a trading platform (or its affiliate) might trade on its own venue.


<sup>34</sup> Exchanges also require certain information from members prior to allowing access to the venue, none of which is required by virtual asset trading platforms. See, e.g., IEX "Exchange Membership and Connectivity," available at <https://iextrading.com/trading/membership/> (requiring Membership Application, User Agreement, Clearing Letter of Guarantee, Form BD, Form U-4, audited financial statements, FOCUS Reports, organizational documents such LLC agreement, and other materials).

<sup>35</sup> itBit reported that it would restrict employee trading in connection with the listing of a new virtual asset on its venue. However, as of September 2018 itBit has only listed one virtual currency: bitcoin.

*First*, a platform might engage in trading in order to make a profit, much like any other trader. *Second*, a trading platform might act as a “market maker,” submitting both buy and sell orders for the same assets in order to promote liquidity – in other words, in order to increase the chances that a customer’s order will execute if another willing buyer or seller does not exist at that moment in time. Those trading objectives are not necessarily exclusive, and indeed can be accomplished by a sophisticated trader at the same time. Such activity is common in the traditional securities marketplace, particularly in broker-operated alternative trading systems (ATSS), but it requires significant commitment to customer protections and transparency to remain in compliance with applicable laws.

**PLATFORM TRADING ON ITS OWN VENUE**

YES	NO	WOULD NOT DISCLOSE
		
		
		
		
		



Trading platforms that engage in proprietary trading on their own venues uniformly told the OAG that their trading desks had no informational or other trading advantage over customers.

The OAG found that significant variation exists in the amount of trading activity attributable to those platform operators. Circle reported that it accounted for less than one percent of the executed volume on its platform Poloniex during the most recent time period reviewed. BitFlyer USA indicated that its own activity accounted for approximately ten percent of the executed volume on its platform. Another, Coinbase, disclosed that almost twenty percent of executed volume on its platform was attributable to its own trading.

Such high levels of proprietary trading raise serious questions about the risks customers face on those platforms. As a general principle, when a significant percentage of the volume in one or more assets on a venue is attributable to one source, customers face the risk that the availability of liquidity in those assets could change, without notice and at any time, including when liquidity is needed most – namely, in times of market volatility or rapid price movement. That certain platforms themselves account for such high levels of activity on their own venues

also calls into question whether the natural market for virtual currencies on those platforms is as robust as customers might believe it to be.

For those platforms that refused to participate in the OAG's Initiative (as well as itBit, which declined to provide any information regarding whether and, to what extent, it traded on its own venue), customers should be aware that a platform could be trading for its own account on its own venue, on an undisclosed basis. Further, those platform operators may have informational and other advantages over traders on their platform. Additionally, customers should be aware that their platform operator might account for a significant percentage of the liquidity on the venue, including a significant percentage of the traded volume of any particular virtual currency.

#### IV. SECURITY, INSURANCE, AND OTHER MEANS OF PROTECTING CONSUMER FUNDS

Customers are rightly concerned about theft, hacking, and fraud. Traditional fiat currency can be physically guarded and recovered if lost. Fraudulent credit card transactions can be reversed. Unauthorized account activity can be halted and remediated through well-understood default rules and systems. Traditional securities are rarely, if ever, stolen. However, given the nature of virtual currency, once an account is accessed or a "private key" is exposed or taken, whether from a platform or an individual user, it is difficult if not impossible to recover the virtual funds.<sup>36</sup> And unlike robbing a bank or stealing a physical wallet, theft of a virtual asset can be accomplished by someone sitting at a computer in a jurisdiction far removed from effective law enforcement.<sup>37</sup> The vulnerability of virtual assets stored on trading platforms is highlighted by several recent high-profile incidents.<sup>38</sup>

In order to more fully understand these issues, the OAG asked virtual asset trading platforms to provide information on several topics, including:

- Security precautions and testing for safeguarding fiat and virtual currency in the custody of platforms;
- Insurance in place to protect against risks to customer funds;

---

<sup>36</sup> A "private key" is a bit of code (typically a long sequence of numbers and letters), which allows the holder of the key to control the virtual currency associated with it. Anyone who gains access to a private key can use it to transfer the virtual currency, which then becomes difficult to recover. For a thorough discussion of the technology underpinning virtual currencies and other "crypto" business applications, see World Bank Fintech Note No.1, "Distributed Ledger Technology (DLT) and Blockchain," (December 2017), available at <http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf>.

<sup>37</sup> See, e.g., International Monetary Fund Staff Discussion Note, "Virtual Currencies and Beyond: Initial Considerations," (January 2016), available at <http://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf> (discussing risks related to the irreversibility of [virtual currency] transactions").

<sup>38</sup> Several of the trading platforms asked to participate in this Initiative have suffered significant incidents resulting in the reported loss of client funds. See, e.g., "Hacked Bitcoin Exchange Bitfinex Will Reduce Balances by 36% to Distribute Losses Amongst All Users," Techcrunch, (Aug. 8, 2016), available at <https://techcrunch.com/2016/08/08/hacked-bitcoin-exchange-bitfinex-will-reduce-balances-by-36-to-distribute-losses-amongst-all-users/>; Coindesk, "Details of \$5 Million Bitstamp Hack Revealed," (Jul. 1, 2015), available at <https://www.coindesk.com/unconfirmed-report-5-million-bitstamp-bitcoin-exchange/>; Forbes, "Crypto Market Drops Amid Rumors of Binance Hack," (Mar. 7, 2018), available at <https://www.forbes.com/sites/jessedamiani/2018/03/07/crypto-market-drops-amid-rumors-of-binance-hack/#a08b8494d000>; Coindesk, "Poloniex Loses 12.3% of its Bitcoins in Latest Bitcoin Exchange Hack," (Mar. 5, 2014), available at <https://www.coindesk.com/poloniex-loses-12-3-bitcoins-latest-bitcoin-exchange-hack/>.

- Audits.

Many platforms expressed reasonable concern to the OAG about publicly detailing their internal processes for securing customer funds. While recognizing that certain aspects of platform operations are indeed sensitive, customers reasonably expect a baseline understanding of what platforms are doing to protect against risks before they trade.

Customers should note that New York’s Department of Financial Services administers regulations regarding the operation of virtual currency businesses in New York. Those regulations impose various obligations on platforms with respect to customer funds, including capital requirements, surety bonds or trust accounts, holding requirements, and other measures. Platforms licensed in New York are not permitted to encumber virtual assets held on behalf of customers.<sup>39</sup>

#### A. SAFEGUARDING VIRTUAL AND FIAT CURRENCY

Few issues are of greater importance to customers of virtual asset trading platforms than the security of the funds entrusted to them. Sophisticated criminals attempt to infiltrate these platforms constantly, and have reportedly stolen billions of dollars’ worth of virtual currency. Once an unauthorized third party gains access to a customer account, those funds can be quickly transferred beyond the reach of law enforcement.

There are several well-understood security practices of interest to customers about which the OAG sought more information.

*First*, the OAG asked platforms whether they required default two-factor authentication of customers. Two-factor authentication is a data security measure that requires a user to input both a password and an additional piece of information in order to log in to an account. The additional piece of information is often a code sent to a phone, or a random number generated by an app or a token. Two-factor authentication helps protect an account even if a password is compromised. While all participating platforms reported to *offer* two-factor authentication for customers in certain circumstances, the better practice is to *require* two-factor identification by default. Default two-factor authentication is the approach taken by all participating platforms except Bitfinex and Tidex. Bittrex and Bitfinex offer an additional option for customers: customers can “whitelist” known IP addresses, and bar access to their account from any other IP address not on the list.<sup>40</sup>

*Second*, most participating platforms purport to keep a high percentage of the virtual currency in their possession in so-called “cold storage.” Cold storage is a security practice wherein the private keys to virtual currency are kept off the internet and thus not susceptible to hacking – in contrast to so-called “hot storage,” where keys are stored on a networked device. Tidex provided no meaningful response.<sup>41</sup>

<sup>39</sup> 29 N.Y.C.R.R. § 200.9(c). The BitLicense regulations can be view in full at <https://www.dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf>.

<sup>40</sup> “Whitelisting” is a practice whereby only known and verified IP addresses may be used to access a customer’s account. Attempted account activity by an unknown IP address is blocked.

<sup>41</sup> Notably, however, it is not possible for customers to verify whether a trading platform is in fact keeping virtual assets in

*Third*, data security cannot be evaluated unless it is put to the test by sophisticated third-parties. Among other things, “penetration testing” can identify security holes in a platform’s information technology and data security infrastructure before a hacker does. Most participating platforms reported to the OAG that they hired independent security consultants to conduct penetration testing and shore up their systems against intrusions. Two participating platforms – Bitfinex and Tidex – did not.

## **B. INSURANCE**

Insurance exists to manage risk. When ordinary New Yorkers engage in certain activities – driving a car, buying a home, opening an ice-cream shop – they are required to carry insurance to mitigate the risk that they, or someone else, will be harmed as a result of that activity. To operate a business of any magnitude, various risks to employees, customers, clients, and others must be insured against. Responsible businesses of all kinds carry insurance.

The use and extent of insurance in connection with the business of holding, exchanging, or transacting in virtual currencies is not well understood. Certain trading platforms, including bitFlyer, the parent company of bitFlyer USA, have been outspoken about their involvement in developing insurance products meant to protect against risks to customer transactions.<sup>42</sup> Coinbase also disclosed to the OAG that it carries insurance to protect against risks to the virtual currency in its custody. However, industry standards have not yet developed around what assets should be insured, against what risk, and at what price.<sup>43</sup> One platform operator expressed to the OAG its opinion that currently available insurance policies concerning virtual currencies do not adequately address issues specific to the storage of virtual assets, including the heightened risk from hacking, and so are inadequate to fully protect customers. itBit refused to provide any information regarding whether carried insurance covering losses of fiat or virtual currency.

In light of the uncertain landscape concerning whether, and how, virtual currencies are insured, customers should demand more information from their trading platforms about how risks to virtual or fiat currency are insured against. For those trading platforms that did not participate in the OAG’s Initiative, as well as itBit, which refused to respond, customers should be aware that those platforms may or may not be insured against the loss of virtual or fiat currency.

## **C. AUDITS**

As a general matter, responsible businesses regularly employ third-parties to review their operations. Audits and other independent reviews provide an added measure of assurance that those aspects of the business under review are proceeding in accordance with meaningful standards. Responsible businesses in any industry should welcome independent third-party review of their operations.

---

sufficiently secure storage, therefore increasing the importance of robust independent auditing, as discussed in this Report.

<sup>42</sup> See Nikkei Asian Review, “Japan’s bitcoin startups to offer insurance for retailers,” (June 30, 2017), available at <https://asia.nikkei.com/Business/Companies/Japan-s-bitcoin-startups-to-offer-insurance-for-retailers>.

<sup>43</sup> See Insurance Journal, “Insurers Begin to Offer Cryptocurrency Theft Cover, Tackling Risks of Growing Sector,” (Feb. 2, 2018), available at <https://www.insurancejournal.com/news/international/2018/02/01/479202.htm>.

The need for independent third-party review is especially acute in the virtual currency markets: the core technology upon which virtual currency is built, and the various applications built on that technology, are new and unproven. Extensive personal customer data is collected and shared, funds (virtual and fiat) are held and exchanged constantly, trading rules and practices are being updated and refined, and insurance or similar safeguards are not universally available or sufficiently robust. Indeed, at the most basic level, many of the companies that hold a significant position in the virtual currency space are new, with unproven track records. The need for independent verification of core policies and procedures is acute.<sup>44</sup>

The OAG asked trading platforms to disclose information regarding audits or other third-party reviews of their policies, procedures, or operations, in order to better understand whether these companies are, at even a basic level, subjecting their operations to oversight and scrutiny. To date, relevant authorities (such as the Financial Accounting Standards Board in the United States) have not developed generally accepted accounting standards for virtual currency. A number of platforms – Bittrex, bitFlyer USA, Bitstamp, Coinbase, Gemini, itBit, and Poloniex (Circle) – reported that they have retained outside firms to conduct audits of their virtual currency holdings using the approaches currently available.

As a general matter, however, the lack of common auditing standards is troubling, given the amounts of customer money (fiat and virtual) held by these platforms, the known data security risks, and increasing integration of virtual currency into other sectors of the financial markets.

**For platforms that declined to participate in the OAG’s Initiative, customers should understand that the business operations of those platforms (including but not limited to financial condition, data security, employee access to trading data, and other issues) may or may not have been reviewed and/or verified.**

## V. ACCESS TO CUSTOMER FUNDS, SUSPENSIONS, AND OUTAGES

The inability of customers to access their fiat and virtual currency is of acute concern to the public. Platforms often fail to detail their procedures for transferring virtual currency from customer accounts to private wallets, or for processing fiat currency withdrawals, or to accomplish those procedures efficiently. This has prompted widespread customer complaints. Compounding these concerns is the reported vulnerability of platforms to being taken offline by bad actors.<sup>45</sup> Trading suspensions and outages are regular occurrences, and customers have been locked out of their accounts and unable to trade. Platforms have exacerbated the problem by not adequately notifying customers of the source or expected duration of outages, properly publicizing what happens to pending orders when trading resumes, or responding to complaints

<sup>44</sup> The regulations promulgated by the New York Department of Financial Services require, among other things, virtual asset trading platforms to undergo reviews and furnish audited financial statements, and to maintain certain books and records.

<sup>45</sup> Platforms regularly face distributed denial of service (“DDoS”) attacks, where the objective is to crash the platform’s website. At least three participating platforms (Bitfinex, Poloniex (Circle), and Bittrex), for example, reported facing DDoS attacks in mid-to-late 2017.

through customer service channels.

Given the continuous, global nature of virtual asset trading, reasonable customers expect their trading platforms to operate seamlessly and predictably. Reliability is especially important at moments of high volume, when market prices change rapidly. Customers also rightly expect to be able reach a platform's customer service representatives. Fast growth in a platform's customer base does not excuse a trading platform's responsibility to ensure that it can handle inevitable problems experienced by customers.<sup>46</sup>

Any electronic trading venue may experience interruptions from time to time. But virtual currency trading platforms holding themselves out as akin to traditional venues of exchange should afford comparable reliability and customer service.

To educate customers about how trading platforms address suspensions of service – including scheduled maintenance, unexpected platform outages, and temporary suspensions of trading – the OAG asked platforms to provide information about the following topics:

- Policies or procedures for suspending trading or delaying pending trades, and the handling of open orders during and immediately following a suspension and/or platform outage; and
- Whether and how the platform alerts customers of trading suspensions, outages, or delays; and
- Whether customers can withdraw or transfer virtual or fiat currency during a suspension or outage.

The OAG also asked platforms to disclose the dates and causes of previous outages, whether customers have access to a log of historical suspensions/outages, and the causes of those incidents.

#### **A. SUSPENSIONS/OUTAGES; USER NOTIFICATION AND TRANSFER OF ASSETS DURING OUTAGES**

The OAG asked trading platforms to describe their policies and procedures for suspending trading or delaying pending trades, and to describe what happens to open orders and currency withdrawals during a trading suspension or platform outage. The OAG also reviewed information regarding whether and how customers are notified of trading suspensions, outages or delays. This is important information for customers, who should understand the circumstances under which their funds (virtual or fiat) could be temporarily unavailable to them for withdrawal or trading.

Platforms differed in how pending trades and currency withdrawals are treated during a trading suspension or outage. Depending upon the reason for the suspension or outage, some platforms cancel pending trades; other do not. On most platforms, customers are not able to withdraw fiat or virtual currency during a suspension or outage, although one platform, bitFlyer USA, noted that customers can withdraw fiat and virtual currency during its daily scheduled

---

<sup>46</sup> See, e.g., Reuters.com, "Cryptocurrency exchanges Coinbase, Bitfinex down," (Dec. 12, 2017) available at [https://www.reuters.com/article/us-bitcoin-exchange/cryptocurrency-exchanges-coinbase-bitfinex-down-idUSKBN1E620E?utm\\_source=applenews](https://www.reuters.com/article/us-bitcoin-exchange/cryptocurrency-exchanges-coinbase-bitfinex-down-idUSKBN1E620E?utm_source=applenews).



maintenance. Given these differences, customers should familiarize themselves with how their trading platform handles open orders during a suspension or outage, and should be sure to understand whether their fiat or virtual currency can be transferred or withdrawn during those times. By and large, however, customers should assume that during periods of suspension or outages, they will not have the ability to trade or withdraw their fiat or virtual assets.

**Customers should also be aware that the platforms that refused to participate in the OAG's Initiative may not have adequate policies and procedures in place governing trading suspensions, outages, or scheduled maintenance, and that customers' virtual or fiat currencies may become unavailable for transfer or withdrawal, without notice.**

## **B. DISCLOSURE OF HISTORICAL OUTAGES**

Given the general inability of customers to trade and/or withdraw fiat and virtual currency during a trading suspension or platform outage, full disclosure of past outages or suspensions, and the reasons for those events, is important to allow customers to evaluate the stability and reliability of a platform, and assess its commitment to transparency. Customers also expect an easy way to understand when any scheduled maintenance will be performed, and platforms should make customers familiar with the extent to which scheduled downtime will impact their ability to trade or withdraw funds.

The OAG asked platforms to provide information about previous outages, including the causes of the incidents, and asked whether that information is made available to customers. While almost every responding platform indicated that it notifies customers in the event of a trading suspension or outage (save for Bitfinex, which declined to answer), only four participating platforms (Coinbase, Gemini, Bitfinex, and Poloniex) publish a history of prior outages. The others (including Bittrex, Tidex, and itBit) do not. At time of publication, HBUS has only recently opened its platform and has yet to experience an outage. Doing so is important for customers in evaluating the historical stability, reliability, and transparency of a venue.

## CONCLUSION: QUESTIONS CUSTOMERS SHOULD ASK A PLATFORM

This Report set out to provide customers with easily-accessible information about virtual asset trading platforms, and to arm customers with the basic questions they should expect every platform to answer:

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 promote transparency and 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, banking regulations or a similar regime – for instance, the New York BitLicense regulations?

This Report does not address all considerations relevant to virtual asset trading platforms or their risks. Nor could it – whether and where customers should trade virtual currencies depends upon the needs and experience of the individual customer. As a general matter, though, customers would do well to avoid platforms that cannot satisfactorily answer the questions posed in this Report.

The OAG remains vigilant when it comes to protecting New York customers from fraud and abusive business practices. The emergent virtual currency marketplace is no different. One of the most important ways the OAG learns about financial abuses is from members of the public who have seen, or been a victim of, fraudulent or abusive conduct. If you have experienced problems with a virtual asset trading platform, or want to report other suspected illegal conduct, please contact the OAG. Complaint forms are available at <https://ag.ny.gov/complaint-forms>.

\* \* \*

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 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 OAG IT and Web Team provided valuable assistance in designing and formatting the interactive and static versions of this report.

## APPENDIX - A

---



STATE OF NEW YORK  
OFFICE OF THE ATTORNEY GENERAL

ERIC T. SCHNEIDERMAN  
ATTORNEY GENERAL

EXECUTIVE DIVISION  
SPECIAL COUNSEL

April 17, 2018

[COMPANY]

*Re: Virtual Markets Integrity Initiative of the New York State Attorney General's Office*

Dear \_\_\_\_\_:

We write on behalf of the New York State Office of the Attorney General (“OAG”) to request the participation of [COMPANY] in OAG’s Virtual Markets Integrity Initiative, which seeks to protect the interests of New York residents who trade virtual currency and related investment products.<sup>1</sup> OAG is asking major virtual currency trading platforms (often referred to as “exchanges”) to respond to a questionnaire addressing key aspects of their operations, including their fee structure, their internal controls, and the measures they take to safeguard funds in customer accounts.<sup>2</sup> Through this Initiative, OAG seeks to increase transparency and accountability in the virtual currency marketplace—and better inform the actions of enforcement agencies, investors, and consumers in this space.

As you know, bitcoin, ether, and other virtual currencies have captured the imagination of millions of people worldwide. Representing a technological advance, a medium of exchange, and an investment opportunity all at once, virtual currencies are inspiring innovators, entrepreneurs, and investors—and are fueling an increasingly diverse ecosystem of companies and applications. But virtual currency is also a highly speculative sector, featuring significant volatility, instability, and risk. Moreover, published reports indicate the sector has attracted fraudsters, market manipulators, and thieves. As the State’s chief law enforcement agency, OAG is responsible for protecting consumers and investors from these bad actors and ensuring the fairness and integrity of New York’s financial markets.<sup>3</sup> *See, e.g.*, N.Y. EXEC. LAW § 63(12); N.Y. GEN. BUS. LAW § 349; N.Y. GEN. BUS. LAW § 352.

<sup>1</sup> As used here and in the enclosed questionnaire, “Virtual Currency” and other terms have the same meanings as set forth in 23 NYCRR § 200.2 (Definitions).

<sup>2</sup> We are aware that certain trading platforms have formal rules barring access in New York and may not have a license to engage in virtual currency business activity in New York. Among other topics, we are asking platforms to describe their measures for restricting trading from prohibited jurisdictions.

<sup>3</sup> This role is separate from, but complementary to, that of New York State’s Department of Financial Services, which established a first-in-the-nation licensing protocol that requires virtual currency trading platforms and other firms engaged in virtual currency business activities to receive approval to operate and follow certain regulatory requirements.

## APPENDIX - A - CONTINUED

---

Page 2 of 2

As with other emerging sectors, the challenge with virtual currency is to prevent fraud and other abuses, safeguard market integrity, and protect individual investors—without stifling legitimate market activity or innovation. OAG’s Virtual Markets Integrity Initiative seeks to advance these objectives by promoting meaningful transparency, accountability, and the opportunity for government agencies, consumer advocates, and investors to compare the policies, procedures, and protections of virtual currency platforms. Sophisticated investors routinely require privately-owned trading venues on which they are considering trading to furnish robust disclosures about their operations, policies, and internal controls so that they can evaluate the risks of trading on a given platform. The enclosed questionnaire asks [COMPANY] to supply similar information, for the benefit of not only professional investors and financial firms, but all consumers who may trade virtual currency on platforms, so that they better understand their operations and the associated risks.

The topics set forth in our questionnaire address fundamental aspects of your operations or issues that have already attracted significant public attention. Indeed, many may be covered in your web disclosures or regulatory filings. They range from your platform’s basic trading rules, to the policies and safeguards you have implemented to prevent conflicts of interest, fraud, and illegality; address the operation of bots; and protection of customer assets from theft and other risks. We will review and assess your responses, compare them with those of other platforms, and disclose certain information in a publicly accessible format.<sup>4</sup> As part of this disclosure, we will identify any platforms that decline to provide meaningfully complete responses.

We kindly ask that you provide detailed and clear responses for each topic, as well as a contact from whom we can seek supplemental information, as necessary. Please complete the enclosed questionnaire and return your responses to our attention no later than May 1, 2018. In the event you have any questions or concerns, please do not hesitate to reach out to us.

Sincerely,



Simon G. Brandler  
Senior Advisor & Special Counsel  
(212) 416-6544  
Simon.Brandler@ag.ny.gov



John D. Castiglione  
Asst. Attorney General, Investor Protection Bureau  
(212) 416-8513  
John.Castiglione@ag.ny.gov

---

<sup>4</sup> You may designate and request confidential treatment for the portion of any response that contains a valid trade secret or may otherwise be exempt from disclosure under New York’s Freedom of Information Law. N.Y. PUB. OFF. LAW §§ 87(2)(a)-(d).

## APPENDIX - B

---



STATE OF NEW YORK  
OFFICE OF THE ATTORNEY GENERAL

### **VIRTUAL MARKETS INTEGRITY INITIATIVE QUESTIONNAIRE**

#### **I. OWNERSHIP AND CONTROL**

1. Provide basic information about your company, including the following:
  - a. Full legal name;
  - b. Legal names of all immediate and ultimate corporate parents, subsidiaries, and Affiliates;
  - c. All directors and officers, including but not limited to Principal Officers, their job titles/roles, and, if applicable, their respective percentages of ownership; and
  - d. All beneficial owners of 5% or more of your company and/or ultimate corporate parent(s), including but not limited to all Principal Stockholders and Principal Beneficiaries.

#### **II. BASIC OPERATION AND FEES**

2. List all domestic and foreign jurisdictions (including U.S. states and territories) from which your platform accepts customers and/or allows transactions. If applicable, describe any measures you take to limit trading on your platform from any other jurisdiction.
3. List each Fiat Currency, Virtual Currency, token, and financial instrument traded on your platform.
4. List all Qualified Custodians, banks, or other institutions, if any, holding customer funds.
5. For each type of fee you charge, including but not limited to fees for deposits/withdrawals, mining, conversions, or other transactions, describe: (a) what the fee covers; (b) its calculation method; and (c) how it is paid. To the extent your platform reduces or waives the fee for certain traders, or has done so in the past, specify the bases for any such reductions (e.g., promotions, discounts for high-volume traders/employees, etc.).
6. Describe your platform's policies and procedures for margin trading, if applicable.
7. Excluding revenue sought or received as customer fees (i.e. fees responsive to item 6 above), detail the source, rationale for, and value in U.S. dollars of any other consideration your platform solicited or received in the past two years. If this includes consideration for listing a Virtual Currency, also describe the circumstances and timing.
8. Describe your respective processes for transferring Virtual Currency from a customer account to a private wallet and, if applicable, withdrawing Fiat Currency from a customer account, including the length of time to complete such a transfer or withdrawal. If processing or execution times vary, provide a range and an average, respectively, for transfers and withdrawals, for the past year. Explain the factors that led to those variations.
9. Describe any services, benefits, or features you provide to customers apart from matching Virtual Currency trades, including but not limited to data feeds, alternative trading interfaces, and access to other trading data, and to whom such service, benefit, or feature is offered.
10. Specify the notional trading volume (in US dollars) on your platform from January 1, 2017 to the present by Virtual Currency, by month.

## APPENDIX - B - CONTINUED

---

### **III. TRADING POLICIES AND PROCEDURES**

11. Describe your order types and process for matching bids and offers, including but not limited to how priority of orders is determined (e.g. first in-first out, order size, order type, etc.).
12. Describe whether and under what circumstances, if any, a customer can arrange or pay for a trade to receive priority over other trades.
13. Describe the method you use to determine the price(s) for exchanging Virtual Currency for Fiat Currency. Explain whether, and at what stage(s) of the transaction, your platform provides any assurance or “locks in” an execution price.
14. Identify the average time and range of times to execute a trade. If execution times vary by currency, order type, or trade type, explain and specify an average and a range for each.
15. Detail the policies, procedures, or technological measures you have in place, if any, concerning the use of “bots” or other forms of automated trading on your platform.
16. Describe any practices, procedures, safeguards, and monitoring your platform has in place to detect, prevent, block, or penalize suspicious trading activity or market manipulation, the types of customer behavior or trading activity that qualifies for such response, and when such measures came into effect.

### **IV. OUTAGES AND OTHER SUSPENSIONS OF TRADING**

17. Describe all policies or procedures for (a) suspending trading or delaying pending trades; (b) completing, canceling, or postponing open orders during a suspension and/or platform outage; and (c) for notifying customers of the suspension, outage, or delay and the rules or contingencies that apply to pending transactions.
18. Describe all policies or procedures you have to allow customers to withdraw or transfer Fiat or Virtual Currency held in their accounts during a suspension or outage.
19. To the extent your platform has in the past suspended trading or experienced an outage, detail: (a) the dates of each such incident; (b) its cause; (c) its duration; (d) the extent to which the incident prevented or delayed customer transfers or withdrawals; and (e) what factors delayed customer transfers or withdrawals.

### **V. INTERNAL CONTROLS**

20. Explain all restrictions or other policies or procedures you maintain concerning whether and how your directors, employees, or Affiliates may trade Virtual Currency on your platform or elsewhere, and when those policies came into effect.
21. State whether your company or, to your knowledge, any Affiliate trades Virtual Currency it owns (a) on your platform; (b) on other platforms; or (c) otherwise.
22. Describe any restrictions or other policies or procedures you maintain to control, limit, or grant access to order flow or other non-public (or not yet public) information related to transactions on your platform (a) within the company and/or (b) to non-employees. If applicable, explain when such policies or procedures came into effect.
23. Identify any person(s) other than your employees with access to your order book or other non-public (or not yet public) information related to bids, asks, or transactions on your platform and the relationship of such person(s) to your company, its officers, directors, or employees.

## APPENDIX - B - CONTINUED

---

24. Describe the scope, frequency, and methodology for any audits or reviews conducted by you or by a third-party of your platform's policies, procedures, operations, or finances, including but not limited to Virtual Currency in your custody.
25. List the third-parties, if any, you engaged to conduct any audit or review responsive to Item 24 above, and the scope of such engagement.

### **VI. PRIVACY AND MONEY LAUNDERING**

26. Identify all categories of personally identifiable information and proof of identity you require before allowing a customer to trade on your platform.
27. Describe all anti-money laundering protocols you have in place, including but not limited to Know Your Customer policies and procedures.
28. Describe your policies, procedures, or other safeguards, if any, to protect the personal information and/or transaction history of customers.

### **VII. PROTECTION AGAINST RISKS TO CUSTOMER FUNDS**

29. Describe the precautions you have in place to safeguard the Fiat Currency, Virtual Currency, or financial instruments in your custody.
30. Explain whether you maintain a capital buffer or working capital to respond to volatility, outages, and other contingencies, the extent of that capital, and how you determine how much of a capital buffer or working capital to maintain.
31. Describe all insurance you carry to protect against any risks to customer funds, what it covers and excludes, and the relevant policy limits, including, if applicable, FDIC deposit insurance.

### **VIII. WRITTEN MATERIALS**

32. Provide a copy of your platform's current terms, conditions, and representations to customers.
33. If applicable, provide a copy of your initial application, including all parts and appendices, and all supplemental submissions, to the New York State Department of Financial Services for a charter or a BitLicense, and for preapproval to trade Virtual Currency.
34. Provide a copy of any written rules or policies you have related to cyber security, privacy, information security, business continuity, disaster recovery, Virtual Currency trading or information use by employees or other persons, or to combating money laundering or fraud.





