Massachusetts Securities Division

Registration, Inspections, Compliance and Examinations Section

▲2018 MID-YEAR NEWSLETTER▲

A Division of William Francis Galvin, Secretary of the Commonwealth

Cybersecurity & Massachusetts Data Privacy Training

On May 2, 2018, the Registration, Inspections, Compliance and Examinations ("RICE") Section of the Massachusetts Securities Division of the Office of the Secretary of the Commonwealth ("Division") hosted a conference on Cybersecurity and Massachusetts Data Privacy. The conference featured presentations by a self-regulatory organization, federal and state regulators, and the private sector. Attendees gained practical advice and learned best practices concerning how to identify cyber risks and develop processes and controls to protect both client data and the firm.

David Kelley, Surveillance Director of FINRA's Kansas City office, presented on effective practices to strengthen controls from a small firm perspective. According to Kelley, small firms often struggle with knowing where to get started when it comes to creating a cybersecurity program. Kelley discussed the most common issues faced by firms and identified resources that can be used to develop efficient processes and controls.

Kelley's Key Points:

- Common sources of cybersecurity issues faced by small firms: phishing emails, customer account takeover, business email compromise, fraudulent wires, ransomware, malware, and using unencrypted email to transmit personal identifying information.
- Best Practices:
  - Regularly conduct risk assessments to identify and address vulnerabilities.
  - Adopt technical controls such as maintaining virus and malware software protection, encrypting emails with personal identifiable information, downloading critical software updates, and testing systems for vulnerabilities.
  - Provide regular cybersecurity training to employees and relevant third parties.
- Resources: The FINRA Small Firm Cybersecurity Checklist available on FINRA's website, the National Institute Standards and Technology ("NIST") Cybersecurity Framework available on NIST's website, and the NASAA cybersecurity checklist for Investment Advisers available on NASAA's website.

Cybersecurity & Massachusetts Data Privacy Panel Discussion: Panelists included Andrea Seidt, Commissioner of Securities for the Ohio Department of Commerce and chair of the NASAA Investment Adviser Section Committee; Kevin Kelcourse, Associate Director of the Securities and Exchange Commission's Office of Compliance Inspections and Examinations, Boston Regional Office; and Kent Sinclair, a private sector practitioner specializing in cybersecurity. The panel was moderated by Carol Foehl, Associate Director of the RICE Section.

The Panelists discussed the following topics:

NASAA's cybersecurity checklist for Investment Advisers address the following five key points:

- *Identify:* Identify an individual responsible for implementing and monitoring its cybersecurity program (even if your firm has one individual) and take an inventory of all devices and sources (such as websites) having access to personal identifiable information.
- *Protect:* Consider your firm's vulnerability in all aspects of its business, including its use of email, devices, cloud services, your firm's website, custodians and other third-party vendors, and encryption methods.
- *Detect:* Use and continually update your firm's anti-virus software and firewalls to detect possible cybersecurity issues.

continued on page 2

In This Issue...

Cybersecurity & Massachusetts Data Privacy Training

continued from page 1

- *Respond:* Implement a plan outlining steps to take in the event of a cybersecurity incident.
- *Recover:* Adopt a disaster recovery plan to continue your firm's business in the event of a cybersecurity incident and consider purchasing cyber-insurance.

Cybersecurity measures adopted by a firm should be proportional to its respective business as measures adopted by larger firms may not be reasonable for smaller firms. However, certain measures should be adopted by all firms. For example, all firms should carefully review the terms of service for vendors and should use secure email servers. In addition, be aware some cloud-based data storage may use or sell the data it stores on your behalf.

As fiduciaries, investment advisers must make a good faith effort to protect client information. In developing an information protection plan, an investment adviser should consider how client information is acquired, used, accessed, stored, shared, and disposed of. Investment advisers must also consider how to protect the information at each stage.

Your feedback: The conference's attendee feedback form requested input from our state-registered investment advisers as to their preferred method of receiving training from the Division. The majority of attendees prefer both webinars and in-person training. The Division is exploring utilizing webinar-based trainings in the future. ▲

Copies of conference materials are available upon request by calling the RICE Section at 617-727-3548 or emailing msd@sec.state.ma.us

Blockchain & Cryptocurrency

The proliferation of financial technology ("FinTech") in the last ten years has resulted in the creation of new securities based on FinTech such as Initial Coin Offerings ("ICOs") using digital coins and digital tokens. Secretary of the Commonwealth of Massachusetts William Galvin recently issued a release cautioning investors about the potential pitfalls surrounding the cryptocurrency Bitcoin.

What is Blockchain?

Blockchain, also referred to as distributed ledger technology, was established in order to create a public ledger to record cryptocurrency transactions. A blockchain is made up of two types of records: transactions and blocks. A block contains the information about multiple transactions, similar to a trade blotter showing all trades across all accounts. As each new block is created, the newest version of the blockchain is distributed across all computers on the network.

> Picture a spreadsheet that is duplicated thousands of times across a network of computers. Then imagine that this network is designed to regularly update this spreadsheet and you have a basic understanding of the blockchain. Information held on a blockchain exists as a shared — and continually reconciled — database. This is a way of using the network that has obvious benefits. The blockchain database isn't stored in any single location, meaning the records it keeps are truly public and easily verifiable. No centralized version of this information exists for a hacker to corrupt. Hosted by millions of computers simultaneously, its data is accessible to anyone on the internet.[1]

The existence of blockchain has led to the creation of a new market of cryptocurrencies. The cryptocurrency market has grown from relatively small numbers in 2013 to a market capitalization of $250 billion dollars as of June 22, 2018.[2]

What are cryptocurrencies?

Cryptocurrencies are a form of exchange and a worldwide payment system that aspire to be used with the same convenience as a national currency like the United States Dollar. These units of exchange, however, exist only in cyberspace and are designed to facilitate online transactions. They allow individuals and institutions to pay each other directly without the use of third party intermediaries like banks or brokerage firms, but do not have a physical form like coins or paper money.

Cryptocurrencies only exist because of what is known as peer-to-peer networks. Peer-to-peer networks are

1 What is Blockchain Technology? A Step-by-Step Guide For Beginners. Retrieved from https://blockgeeks.com/guides/what-is-blockchain-technology/

2 Retrieved from https://coinmarketcap.com/

comprised of computers connected through the Internet that can share files without the use of a central server. This is known as distributed computing. Just as other file sharing programs use this technology to distribute millions of files, cryptocurrencies use the same technology to create, execute and approve transactions by sharing files. These cryptocurrency transactions are recorded using blockchain technology.

Where does cryptocurrency come from and how are they created?

Bitcoin, a type of cryptocurrency is created through a process called mining. This is accomplished by harnessing the processing power of computers on a peer-to-peer network. These computers compete against each other to solve complex mathematical equations that verify the security of the blockchain and the authenticity of the cryptocurrency transaction. The computers that win these competitions are rewarded in cryptocurrency. Other tokens are created through ICOs, discussed below, on already existing blockchain (i.e. Ethereum) with a couple of hundred lines of code.

Valuation of Cryptocurrency

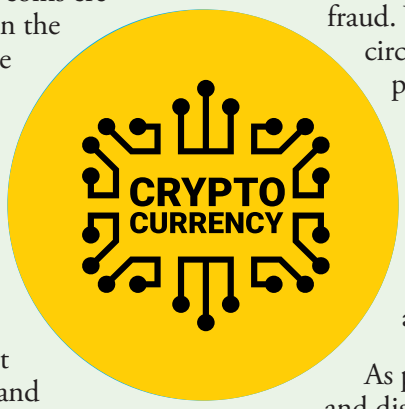
The value of cryptocurrency is determined by the laws of supply and demand that affect the prices of other units of exchange. However, they have not been accepted as a mainstream form of payment. It is important to consider whether there is a "bubble" in the prices of cryptocurrencies. When cryptocurrencies are the object of pure speculation and not long term investment, this might be a warning sign. For example, a recent paper published by a finance professor and graduate student at the University of Texas indicates that a "concentrated campaign of price manipulation may have accounted for at least half of the increase in the price of Bitcoin and other big cryptocurrencies last year."[3]

Secretary Galvin's recent alert has pointed out several of the pitfalls in buying and selling products like cryptocurrencies. His caution to investors emphasizes that the public should be wary of unscrupulous actors who have entered this marketplace. Many of the wallets (where the public can deposit their cryptocurrencies) and even cryptocurrency exchanges have been compromised by hackers leaving some investors with substantial losses. ▲

3 Bitcoin's Price Was Artificially Inflated, Fueling Skyrocketing Value, Researchers Say. Retrieved from https://www.nytimes.com/2018/06/13/technology/bitcoin-price-manipulation.html

INITIAL COIN OFFERINGS ("ICOs") & RECENT ICO ENFORCEMENT ACTIONS

Cryptocurrency, or digital currency, is often marketed as digital coins or digital tokens. With a minimal amount of computer knowledge anyone can create coins and attempt to conduct an ICO. Many of the coins created are illiquid, cannot be easily traded on the secondary market, can only be used on the issuer's platform, and may have no inherent use or value. Because of the relative ease of conducting an ICO, there has been a recent spate of individuals seeking to raise capital through ICOs. These offerings are often unregistered securities being offered by unregistered agents whose companies are not registered. The Division has created a task force to protect Massachusetts investors from individuals and companies not complying with the Massachusetts Uniform Securities Act who are trying to take advantage of investors using this new technology.



What are ICOs?

ICOs occur when investors are solicited to exchange a government-backed currency or a cryptocurrency in return for a digital coin or token. ICOs may present new avenues of raising capital, however, there are many opportunities for fraud and market manipulation.

Considerations for and impact on state-registered investment advisers

The ICO market is rampant with opportunities for fraud. While each review is based on facts and circumstances, the Division has taken the position that there is a strong presumption that the sale of an ICO that is not registered or exempt from registration is a violation of state securities law. The Division has full authority to enforce fraud violations in connection with ICOs involving Massachusetts residents and entities.

As part of the ICO, the issuer will create and distribute a whitepaper. A whitepaper is analogous to a private placement memorandum, or a prospectus of a more traditional security. Recently, in an attempt to capitalize on the ICO hype, whitepapers have evolved from technical explanations to being shorter, cut and paste boiler plate disclosures with more buzzwords and blockchain jargon.

ICO Enforcement Action

On January 17, 2018, the Division filed an administra-

continued on page 4

tive complaint against a local ICO issuer. The complaint charged the issuer, a Massachusetts resident, and his company, with an unregistered offering of securities in the Commonwealth and unregistered agent activity. The issuer marketed and sold their tokens through an ICO. Proceeds from the token sale were to be invested in a portfolio of cryptocurrencies, while hedging the volatility of the cryptocapital market by investing in real estate "flips". The issuer would then use the profits of the cryptocurrency and real estate investments to pay a quarterly dividend per token.

As of the date of the filing of the administrative complaint, the issuer alleged to have raised $3.1 million. The Division took the position that the issuer's tokens were investment contracts per the *Howey* test because investors in the issuer invested in a common enterprise, the funds were pooled to invest in cryptocurrencies and real estate, and the investors had an expectation of profit (dividends), which were based on the efforts of the issuer. The administrative complaint seeks to make the issuer cease and desist from offering unregistered securities in the Commonwealth, offer rescission to investors, and pay an administrative fine. This was the first state enforcement action against an ongoing ICO.

Enforcement Section's ICO Sweep

On March 27, 2018, the Division ordered five firms, with ties to Massachusetts, to halt the offering and selling of unregistered securities in Massachusetts. These five firms were independently conducting their own ICO by offering unique cryptocurrencies. The Division took the position that the tokens issued as part of each ICO were investment contracts per the *Howey* test, and needed to be registered or exempt from registration. All five firms were ordered to cease and desist from offering and selling unregistered securities and to offer rescission to anyone sold unregistered securities.

NASAA's ICO Sweep

The North American Securities Administrators Association ("NASAA"), in conjunction with NASAA members from more than 40 jurisdictions throughout North America, conducted a coordinated series of enforcement actions on companies and representatives who fraudulently engaged in ICO and cryptocurrency related products in May 2018. The sweep led to nearly 70 inquiries and investigations and 35 pending or completed enforcement actions. Joseph P. Borg, NASAA President and Director of the Alabama Securities Commission stated, "[t]he persistently expanding exploitation of the crypto ecosystem by fraudsters is a significant threat to Main Street investors in the United States and Canada, and NASAA members are committed to combating this threat." The purpose of the sweep was not only to crack down on fraudulent offerings but to raise public awareness regarding the risks of ICOs and cryptocurrency related products. ▲

LPL Multi-State Settlement

On June 12, 2018, the Division entered a Consent Order with LPL Financial, LLC based, in part, on LPL's failure to establish and maintain reasonable policies and procedures to prevent the sale of unregistered, non-exempt securities to its Massachusetts customers. Pursuant to the Consent Order, LPL will offer to repurchase or pay damages to Massachusetts investors who were sold unregistered, non-exempt securities as far back as October 2006. In addition, LPL will engage a third-party consultant to conduct a full assessment of LPL's "Blue Sky" compliance and supervisory safeguards, and pay a fine of $499,000 in Massachusetts.

The Division's Consent Order is part of a coordinated multistate investigation led by the Division and the Alabama Securities Commission, involving all fifty states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands. ▲