Faculty:
Cryptocurrency: Valuation Issues and Market Volatility

Kevin Madura is a senior vice president with AlixPartners, LLP in Washington, D.C., and is a technologist with a specialization in cybersecurity, working to apply the power of technology to secure and accelerate businesses in the digital era. He has worked in both public and private sectors to solve technical and security challenges, with clients ranging from the Department of Defense to large corporations. In addition to strategic guidance, Mr. Madura advises law firm clients in the areas of computer forensics, cryptocurrencies and cryptography. He previously was a cybersecurity consultant with IBM and an IT systems engineer with Unleashed Technologies. Mr. Madura received his B.S. in computer science from the University of Maryland College Park and his Master's in technology management from Georgetown University.

Laurel Loomis Rimon is a partner with O'Melveny & Myers LLP in Washington, D.C. Drawing on her almost 25-year career in government service, which included high-level positions at the Department of Justice, Consumer Finance Protection Bureau and Department of Homeland Security, she advises financial institutions, fintech companies and government entities on compliance issues, enforcement actions, and internal and government investigations. Before joining O'Melveny, Ms. Rimon served for more than 15 years as an Assistant U.S. Attorney and DOJ trial attorney, including tenure as head of Litigation for DOJ's Asset Forfeiture and Money Laundering Section, where she litigated complex criminal and civil money laundering and other financial crimes. As a federal prosecutor, she successfully led the earliest federal prosecution involving virtual currency, the money laundering and money transmitting prosecution of the "e-gold" enterprise, providing her with an early appreciation of the intersection of financial services regulation and digital assets. Ms. Rimon's government experience also includes serving as an Assistant Deputy Enforcement Director for the Office of Enforcement at the Consumer Financial Protection Bureau, leading complex and sensitive investigations of bank and nonbank subjects that included large banks, private educational institutions and mortgage loan companies. She leverages this deep regulatory and enforcement experience to help her financial institution clients develop compliance programs and respond to DOJ and CFPB inquiries and enforcement actions regarding anti-money laundering, the Bank Secrecy Act and the Consumer Financial Protection Act. She also advises cutting-edge fintech companies in the payments and cryptocurrency spaces on financial regulatory compliance and enforcement matters relating to AML, sanctions and consumer protection. Ms. Rimon has unique expertise in the development of whistleblower compliance programs and investigations after having led the Department of Homeland Security's whistleblower protection and investigations program. She received her B.A. from the University of California at Berkeley and her J.D. from Southwestern Law School.

Alan R. Rosenberg is partner with Markowitz Ringel Trusty + Hartog in Miami, where he represents bankruptcy trustees, creditors, debtors and other parties-in-interest in all aspects of insolvency proceedings and bankruptcy-related litigation, including, but not limited to, the sale of bankruptcy estate assets and the pursuit and defense of avoidance actions and other litigation claims. In addition to his bankruptcy practice, he also represents individual and corporate clients in a wide variety of commercial litigation claims and real estate transactions. In his free time, Mr. Rosenberg enjoys learning about cryptocurrency and blockchain technology, and has been published several times on the subject. He is listed as a *Florida Super Lawyer* "Rising Star" for 2017-21 and a *Florida Legal Elite* "Up and Comer" from 2018-20, and in 2020 was honored as one of ABI's "40 Under 40." Mr. Rosenberg received his B.S.B.A. in finance in 2008 from the University of Florida and his J.D. *cum laude* from the University of Miami in 2011.

Scott Rothman is a partner with Beechwood Capital Advisors, Inc. in Millburn, N.J., and has more than 20 years of banking, capital markets and consulting experience. Prior to joining Beechwood in March 2019, he had co-founded JFD Securities in 2002 (which sold in 2016), a registered broker-dealer providing option trading strategies and derivative execution to global hedge funds, asset managers and mutual funds. Mr. Rothman previously held management, sales and investment positions in several companies in the digital assets and blockchain, fintech, health care, gaming, foreign exchange and real estate industries. He holds Series 4, Series 7, Series 24, Series 55 and Series 63 FINRA licenses. Mr. Rothman received his B.A. from Pennsylvania State University and his M.B.A. from Rutgers University.

Additional Resources:
Cryptocurrency: Valuation Issues and Market Volatility

- Bitcoin private keys: https://getbitcoinclarity.com/blog/2020/05/16/what-is-a-bitcoin-private-key
- Intro to keys: https://support.blockchain.com/hc/en-us/articles/360000951966-Public-and-private-keys
- Fed reserve on stablecoins: https://www.federalreserve.gov/newsevents/speech/quarles20210628a.htm
- WSJ article on potential regulation: https://www.wsj.com/articles/risks-of-crypto-stablecoins-attract-attention-of-yellen-fed-and-sec-11626537601
- Summary of the digitization of the dollar: https://unexpected-values.com/crypto-dollars/
- An introduction to Decentralized Finance: https://blog.coinbase.com/a-beginners-guide-to-decentralized-finance-defi-574c68ff43c4

23 CRR-NY 200.2
NY-CRR

OFFICIAL COMPILATION OF CODES, RULES AND REGULATIONS OF THE STATE OF NEW YORK
TITLE 23. FINANCIAL SERVICES
CHAPTER I. REGULATIONS OF THE SUPERINTENDENT OF FINANCIAL SERVICES
PART 200. VIRTUAL CURRENCIES

23 CRR-NY 200.2
23 CRR-NY 200.2

200.2 Definitions.

For purposes of this Part only, the following definitions shall apply:

(a) *affiliate* means any person that directly or indirectly controls, is controlled by, or is under common control with, another person;

(b) *cyber security event* means any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt, or misuse a licensee's electronic systems or information stored on such systems;

(c) *department* means the New York State Department of Financial Services;

(d) *exchange service* means the conversion or exchange of fiat currency or other value into virtual currency, the conversion or exchange of virtual currency into fiat currency or other value, or the conversion or exchange of one form of virtual currency into another form of virtual currency;

(e) *fiat currency* means government-issued currency that is designated as legal tender in its country of issuance through government decree, regulation, or law;

(f) *licensee* means any person duly licensed by the superintendent pursuant to this Part;

(g) *New York* means the State of New York;

(h) *New York resident* means any person that resides, is located, has a place of business, or is conducting business in New York;

(i) *person* means an individual, partnership, corporation, association, joint stock association, trust, or other entity, however organized;

(j) *prepaid card* means an electronic payment device that:

(1) is usable at a single merchant or an affiliated group of merchants that share the same name, mark, or logo, or is usable at multiple, unaffiliated merchants or service providers;

(2) is issued in and for a specified amount of fiat currency;

(3) can be reloaded in and for only fiat currency, if at all;

(4) is issued and/or reloaded on a prepaid basis for the future purchase or delivery of goods or services;

(5) is honored upon presentation; and

(6) can be redeemed in and for only fiat currency, if at all;

(k) *principal officer* means an executive officer of an entity, including, but not limited to, the chief executive, financial, operating, and compliance officers, president, general counsel, managing partner, general partner, controlling partner, and trustee, as applicable;

(l) *principal stockholder* means any person that directly or indirectly owns, controls, or holds with power to vote 10 percent or more of any class of outstanding capital stock or other equity interest of an entity or possesses the power to direct or cause the direction of the management or policies of the entity;

(m) *principal beneficiary* means any person entitled to 10 percent or more of the benefits of a trust;

(n) *qualified custodian* means a bank, trust company, national bank, savings bank, savings and loan association, Federal savings association, credit union, or Federal credit union in the State of New York, subject to the prior approval of the superintendent. To the extent applicable, terms used in this definition shall have the meaning ascribed by the Banking Law;

(o) *transmission* means the transfer, by or through a third party, of virtual currency from a person to a person, including the transfer from the account or storage repository of a person to the account or storage repository of a person;

(p) *virtual currency* means any type of digital unit that is used as a medium of exchange or a form of digitally stored value. virtual currency shall be broadly construed to include digital units of exchange that: have a centralized repository or administrator; are decentralized and have no centralized repository or administrator; or may be created or obtained by computing or manufacturing effort. *Virtual currency* shall not be construed to include any of the following:

(1) digital units that:

(i) are used solely within online gaming platforms;

(ii) have no market or application outside of those gaming platforms;

(iii) cannot be converted into, or redeemed for, fiat currency or virtual currency; and

(iv) may or may not be redeemable for real-world goods, services, discounts, or purchases;

(2) digital units that can be redeemed for goods, services, discounts, or purchases as part of a customer affinity or rewards program with the issuer and/or other designated merchants or can be redeemed for digital units in another customer affinity or rewards program, but cannot be converted into, or redeemed for, fiat currency or virtual currency; or

(3) digital units used as part of prepaid cards;

(q) *virtual currency business activity* means the conduct of any one of the following types of activities involving New York or a New York resident:

(1) receiving virtual currency for transmission or transmitting virtual currency, except where the transaction is undertaken for non-financial purposes and does not involve the transfer of more than a nominal amount of virtual currency;

(2) storing, holding, or maintaining custody or control of virtual currency on behalf of others;

(3) buying and selling virtual currency as a customer business;

(4) performing exchange services as a customer business; or

(5) controlling, administering, or issuing a virtual currency.

The development and dissemination of software in and of itself does not constitute virtual currency business activity.

23 CRR-NY 200.2
Current through September 30, 2020

23 CRR-NY 200.2
NY-CRR

OFFICIAL COMPILATION OF CODES, RULES AND REGULATIONS OF THE STATE OF NEW YORK
TITLE 23. FINANCIAL SERVICES
CHAPTER I. REGULATIONS OF THE SUPERINTENDENT OF FINANCIAL SERVICES
PART 200. VIRTUAL CURRENCIES

23 CRR-NY 200.2
23 CRR-NY 200.2

200.2 Definitions.

For purposes of this Part only, the following definitions shall apply:

(a) *affiliate* means any person that directly or indirectly controls, is controlled by, or is under common control with, another person;

(b) *cyber security event* means any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt, or misuse a licensee's electronic systems or information stored on such systems;

(c) *department* means the New York State Department of Financial Services;

(d) *exchange service* means the conversion or exchange of fiat currency or other value into virtual currency, the conversion or exchange of virtual currency into fiat currency or other value, or the conversion or exchange of one form of virtual currency into another form of virtual currency;

(e) *fiat currency* means government-issued currency that is designated as legal tender in its country of issuance through government decree, regulation, or law;

(f) *licensee* means any person duly licensed by the superintendent pursuant to this Part;

(g) *New York* means the State of New York;

(h) *New York resident* means any person that resides, is located, has a place of business, or is conducting business in New York;

(i) *person* means an individual, partnership, corporation, association, joint stock association, trust, or other entity, however organized;

(j) *prepaid card* means an electronic payment device that:

(1) is usable at a single merchant or an affiliated group of merchants that share the same name, mark, or logo, or is usable at multiple, unaffiliated merchants or service providers;

(2) is issued in and for a specified amount of fiat currency;

(3) can be reloaded in and for only fiat currency, if at all;

(4) is issued and/or reloaded on a prepaid basis for the future purchase or delivery of goods or services;

(5) is honored upon presentation; and

(6) can be redeemed in and for only fiat currency, if at all;

(k) *principal officer* means an executive officer of an entity, including, but not limited to, the chief executive, financial, operating, and compliance officers, president, general counsel, managing partner, general partner, controlling partner, and trustee, as applicable;

(l) *principal stockholder* means any person that directly or indirectly owns, controls, or holds with power to vote 10 percent or more of any class of outstanding capital stock or other equity interest of an entity or possesses the power to direct or cause the direction of the management or policies of the entity;

(m) *principal beneficiary* means any person entitled to 10 percent or more of the benefits of a trust;

(n) *qualified custodian* means a bank, trust company, national bank, savings bank, savings and loan association, Federal savings association, credit union, or Federal credit union in the State of New York, subject to the prior approval of the superintendent. To the extent applicable, terms used in this definition shall have the meaning ascribed by the Banking Law;

(o) *transmission* means the transfer, by or through a third party, of virtual currency from a person to a person, including the transfer from the account or storage repository of a person to the account or storage repository of a person;

(p) *virtual currency* means any type of digital unit that is used as a medium of exchange or a form of digitally stored value. virtual currency shall be broadly construed to include digital units of exchange that: have a centralized repository or administrator; are decentralized and have no centralized repository or administrator; or may be created or obtained by computing or manufacturing effort. *Virtual currency* shall not be construed to include any of the following:

(1) digital units that:

(i) are used solely within online gaming platforms;

(ii) have no market or application outside of those gaming platforms;

(iii) cannot be converted into, or redeemed for, fiat currency or virtual currency; and

(iv) may or may not be redeemable for real-world goods, services, discounts, or purchases;

(2) digital units that can be redeemed for goods, services, discounts, or purchases as part of a customer affinity or rewards program with the issuer and/or other designated merchants or can be redeemed for digital units in another customer affinity or rewards program, but cannot be converted into, or redeemed for, fiat currency or virtual currency; or

(3) digital units used as part of prepaid cards;

(q) *virtual currency business activity* means the conduct of any one of the following types of activities involving New York or a New York resident:

(1) receiving virtual currency for transmission or transmitting virtual currency, except where the transaction is undertaken for non-financial purposes and does not involve the transfer of more than a nominal amount of virtual currency;

(2) storing, holding, or maintaining custody or control of virtual currency on behalf of others;

(3) buying and selling virtual currency as a customer business;

(4) performing exchange services as a customer business; or

(5) controlling, administering, or issuing a virtual currency.

The development and dissemination of software in and of itself does not constitute virtual currency business activity.

23 CRR-NY 200.2
Current through September 30, 2020

Public Statement

Remarks Before the Aspen Security Forum

Chair Gary Gensler

Aug. 3, 2021

Thank you for that kind introduction. It's good to join the Aspen Security Forum.

As is customary, I'd like to note that my views are my own, and I'm not speaking on behalf of the Commission or the SEC staff.

Some might wonder: What does the SEC have to do with crypto?

Further, why did an organization like the Aspen Security Forum ask me to speak about crypto's intersection with national security?

Let me start at the beginning.

It was Halloween night 2008, in the middle of the financial crisis, when Satoshi Nakamoto published an eight-page paper[1] on a cypherpunk mailing list that'd been run by cryptographers since 1992.[2]

Nakamoto — we still don't know who she, he, or they were — wrote, "I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party."[3]

Nakamoto had solved two riddles that had dogged these cryptographers and other technology experts for a couple of decades: first, how to move something of value on the internet without a central intermediary; and relatedly, how to prevent the "double-spending" of that valuable digital token.

Subsequently, his innovation spurred the development of crypto assets and the underlying blockchain technology.

Based upon Nakamoto's innovation, about a dozen years later, the crypto asset class has ballooned. As of Monday, this asset class purportedly is worth about $1.6 trillion, with 77 tokens worth at least $1 billion each and 1,600 with at least a $1 million market capitalization.[4]

Before starting at the SEC, I had the honor of researching, writing, and teaching about the intersection of finance and technology at the Massachusetts Institute of Technology. This included courses on crypto finance, blockchain technology, and money.

In that work, I came to believe that, though there was a lot of hype masquerading as reality in the crypto field, Nakamoto's innovation is real. Further, it has been and could continue to be a catalyst for change in the fields of finance and money.[5]

At its core, Nakamoto was trying to create a private form of money with no central intermediary, such as a central bank or commercial banks.

We already live in an age of digital public monies — the dollar, euro, sterling, yen, yuan. If that wasn't obvious before the pandemic, it has become eminently clear over the last year that we increasingly transact online.

Such public fiat monies fulfill the three functions of money: a store of value, unit of account, and medium of exchange.

No single crypto asset, though, broadly fulfills all the functions of money.

Primarily, crypto assets provide digital, scarce vehicles for speculative investment. Thus, in that sense, one can say they are highly speculative stores of value.

These assets haven't been used much as a unit of account.

We also haven't seen crypto used much as a medium of exchange. To the extent that it is used as such, it's often to skirt our laws with respect to anti-money laundering, sanctions, and tax collection. It also can enable extortion via ransomware, as we recently saw with Colonial Pipeline.

With the advent of the internet age and the movement from physical money to digital money several decades ago, nations around the globe layered various public policy goals over our digital public money system.

As a policy matter, I'm technology-neutral.

As a personal matter, I wouldn't have gone to MIT if I weren't interested in how technology can expand access to finance and contribute to economic growth.

But I am anything but public policy-neutral. As new technologies come along, we need to be sure we're achieving our core public policy goals.

In finance, that's about protecting investors and consumers, guarding against illicit activity, and ensuring financial stability.

So how does the SEC fit into all this?

The SEC has a three-part mission — to protect investors, facilitate capital formation, and maintain fair, orderly, and efficient markets in between them. We focus on financial stability as well. But at our core, we're about investor protection.

If you want to invest in a digital, scarce, speculative store of value, that's fine. Good-faith actors have been speculating on the value of gold and silver for thousands of years.

Right now, we just don't have enough investor protection in crypto. Frankly, at this time, it's more like the Wild West.

This asset class is rife with fraud, scams, and abuse in certain applications. There's a great deal of hype and spin about how crypto assets work. In many cases, investors aren't able to get rigorous, balanced, and complete information.

If we don't address these issues, I worry a lot of people will be hurt.

First, many of these tokens are offered and sold as securities.

There's actually a lot of clarity on that front. In the 1930s, Congress established the definition of a security, which included about 20 items, like stock, bonds, and notes. One of the items is an investment contract.

The following decade, the Supreme Court took up the definition of an investment contract. This case said an investment contract exists when "a person invests his money in a common enterprise and is led to expect profits solely from the efforts of the promoter or a third party."[6] The Supreme Court has repeatedly reaffirmed this Howey Test.

Further, this is but one of many ways we determine whether tokens must comply with the federal securities laws.

I think former SEC Chairman Jay Clayton said it well when he testified in 2018: “To the extent that digital assets like [initial coin offerings, or ICOs] are securities — and I believe every ICO I have seen is a security — we have jurisdiction, and our federal securities laws apply.”[7]

I find myself agreeing with Chairman Clayton. You see, generally, folks buying these tokens are anticipating profits, and there’s a small group of entrepreneurs and technologists standing up and nurturing the projects. I believe we have a crypto market now where many tokens may be unregistered securities, without required disclosures or market oversight.

This leaves prices open to manipulation. This leaves investors vulnerable.

Over the years, the SEC has brought dozens of actions in this area,[8] prioritizing token-related cases involving fraud or other significant harm to investors. We haven’t yet lost a case.

Moreover, there are initiatives by a number of platforms to offer crypto tokens or other products that are priced off of the value of securities and operate like derivatives.

Make no mistake: It doesn’t matter whether it’s a stock token, a stable value token backed by securities, or any other virtual product that provides synthetic exposure to underlying securities. These products are subject to the securities laws and must work within our securities regime.

I’ve urged staff to continue to protect investors in the case of unregistered sales of securities.

Next, I’d like to discuss crypto trading platforms, lending platforms, and other “decentralized finance” (DeFi) platforms.

The world of crypto finance now has platforms where people can trade tokens and other venues where people can lend tokens. I believe these platforms not only can implicate the securities laws; some platforms also can implicate the commodities laws and the banking laws.

A typical trading platform has more than 50 tokens on it. In fact, many have well in excess of 100 tokens. While each token’s legal status depends on its own facts and circumstances, the probability is quite remote that, with 50 or 100 tokens, any given platform has zero securities.

Moreover, unlike other trading markets, where investors go through an intermediary like the New York Stock Exchange, people can trade on crypto trading platforms without a broker — 24 hours a day, 7 days a week, from around the globe.

Further, while many overseas platforms state they don’t allow U.S. investors, there are allegations that some unregulated foreign exchanges facilitate trading by U.S. traders who are using virtual private networks, or VPNs.[9]

The American public is buying, selling, and lending crypto on these trading, lending, and DeFi platforms, and there are significant gaps in investor protection.

Make no mistake: To the extent that there are securities on these trading platforms, under our laws they have to register with the Commission unless they meet an exemption.

Make no mistake: If a lending platform is offering securities, it also falls into SEC jurisdiction.

Next, I’d like to turn to stable value coins, which are crypto tokens pegged or linked to the value of fiat currencies.

Many of you have heard about Facebook’s efforts to stand up a stablecoin called Diem (formerly known as Libra).

Due to the global reach of Facebook’s platform, this has gotten a lot of attention from central bankers and regulators. This is not only due to general policies and concerns with crypto, but also due to Diem’s potential impact on monetary policy, banking policy, and financial stability.

Maybe less well known to this audience, though, is that we already have an existing stablecoin market worth $113 billion,[10] including four large stablecoins — some of which have been around for seven years.

These stablecoins are embedded in crypto trading and lending platforms.

How do you trade crypto-to-crypto? Usually, somebody uses stablecoins.

In July, nearly three-quarters of trading on all crypto trading platforms occurred between a stablecoin and some other token.[11]

Thus, the use of stablecoins on these platforms may facilitate those seeking to sidestep a host of public policy goals connected to our traditional banking and financial system: anti-money laundering, tax compliance, sanctions, and the like. This affects our national security, too.

Further, these stablecoins also may be securities and investment companies. To the extent they are, we will apply the full investor protections of the Investment Company Act and the other federal securities laws to these products.

I look forward to working with my colleagues on the President's Working Group on Financial Markets on these matters.[12]

Next, I want to turn to investment vehicles providing exposure to crypto assets. Such investment vehicles already exist, with the largest among them having been around for eight years and worth more than $20 billion.[13] Also, there are a number of mutual funds that invest in Bitcoin futures on the Chicago Mercantile Exchange (CME).

I anticipate that there will be filings with regard to exchange-traded funds (ETFs) under the Investment Company Act ('40 Act). When combined with the other federal securities laws, the '40 Act provides significant investor protections.

Given these important protections, I look forward to the staff's review of such filings, particularly if those are limited to these CME-traded Bitcoin futures.

The final policy area has to do with custody of crypto assets. The SEC is seeking comment on crypto custody arrangements by broker-dealers and relating to investment advisers.[14] Custody protections are key to preventing theft of investor assets, and we will be looking to maximize regulatory protections in this area.

Before I conclude, I'd like to note we have taken and will continue to take our authorities as far as they go.

Certain rules related to crypto assets are well-settled. The test to determine whether a crypto asset is a security is clear.

There are some gaps in this space, though: We need additional Congressional authorities to prevent transactions, products, and platforms from falling between regulatory cracks. We also need more resources to protect investors in this growing and volatile sector.

We stand ready to work closely with Congress, the Administration, our fellow regulators, and our partners around the world to close some of these gaps.

In my view, the legislative priority should center on crypto trading, lending, and DeFi platforms. Regulators would benefit from additional plenary authority to write rules for and attach guardrails to crypto trading and lending.

Right now, large parts of the field of crypto are sitting astride of — not operating within — regulatory frameworks that protect investors and consumers, guard against illicit activity, ensure for financial stability, and yes, protect national security.

Standing astride isn't a sustainable place to be. For those who want to encourage innovations in crypto, I'd like to note that financial innovations throughout history don't long thrive outside of our public policy frameworks.

At the heart of finance is trust. And at the heart of trust in markets is investor protection. If this field is going to continue, or reach any of its potential to be a catalyst for change, we better bring it into public policy frameworks.

Thank you. I look forward to your questions.

[1] *See* Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," *available at* https://bitcoin.org/bitcoin.pdf.

[2] *See* Haseeb Qureshi "The Cypherpunks" (Dec. 29, 2019), *available at* https://nakamoto.com/the-cypherpunks/.

[3] *See* "Bitcoin P2P e-cash paper" (Oct. 31, 2008), *available at* https://satoshi.nakamotoinstitute.org/emails/cryptography/1/.

[4] Numbers as of Aug. 2, 2021. *See* CoinMarketCap, *available at* www.coinmarketcap.com. Crypto asset figures are not audited or reported to regulatory authorities.

[5] *See* Michael Casey, Jonah Crane, Gary Gensler, Simon Johnson, and Neha Narula, "The Impact of Blockchain Technology on Finance: A Catalyst for Change" (2018), *available at* https://www.sipotra.it/wp-content/uploads/2018/07/The-Impact-of-Blockchain-Technology-on-Finance-A-Catalyst-for-Change.pdf.

[6] *See* SEC v. Howey Co., 328 U.S. 293 (1946), "Framework for 'Investment Contract' Analysis of Digital Assets," *available at* https://supreme.justia.com/cases/federal/us/328/293/.

[7] *See* Jay Clayton, Testimony United States Senate Committee on Banking, Housing, And Urban Affairs, "Virtual Currencies: The Oversight Role of the U.S. Securities and Exchange Commission and the U.S. Commodity Futures Trading Commission" (Feb. 6, 2018), *available at* https://www.banking.senate.gov/hearings/virtual-currencies-the-oversight-role-of-the-us-securities-and-exchange-commission-and-the-us-commodity-futures-trading-commission (see approx. 32:00 mark).

[8] *See* Cornerstone Research, "Cornerstone Research Report Shows SEC Establishes Itself as a Key U.S. Cryptocurrency Regulator" (May 11, 2021), *available at* https://www.cornerstone.com/Publications/Press-Releases/Cornerstone-Research-Report-Shows-SEC-Establishes-Itself-as-a-Key-U-S-Cryptocurrency-Regulator.

[9] *See* Alexander Osipovich, "U.S. Crypto Traders Evade Offshore Exchange Bans" (July 30, 2021), *available at* https://www.wsj.com/articles/u-s-crypto-traders-evade-offshore-exchange-bans-11627637401.

[10] Numbers as of Aug. 1. *See* The Block, "Total Stablecoin Supply," *available at* https://www.theblockcrypto.com/data/decentralized-finance/stablecoins.

[11] *See* The Block, "Share of Trade Volume by Pair Denomination," *available at* https://www.theblockcrypto.com/data/crypto-markets/spot.

[12] *See* "Readout of the Meeting of the President's Working Group on Financial Markets to Discuss Stablecoins" (July 19, 2021), *available at* https://home.treasury.gov/news/press-releases/jy0281.

[13] *See* Grayscale® Bitcoin Trust, *available at* https://grayscale.com/products/grayscale-bitcoin-trust/.

[14] *See* Securities and Exchange Commission, "Staff Statement on WY Division of Banking's 'NAL on Custody of Digital Assets and Qualified Custodian Status'" (Nov. 9, 2020), *available at* https://www.sec.gov/news/public-statement/statement-im-finhub-wyoming-nal-custody-digital-assets. *See* Securities and Exchange Commission, "SEC Issues Statement and Requests Comment Regarding the Custody of Digital Asset Securities by Special Purpose Broker-Dealers" (Dec. 23, 2020), *available at* https://www.sec.gov/news/press-release/2020-340.

BEECHWOOD
CAPITAL ADVISORS

August 2021

www.beechwoodcapitaladvisors.com

Capital Raising and M&A for the Middle Market

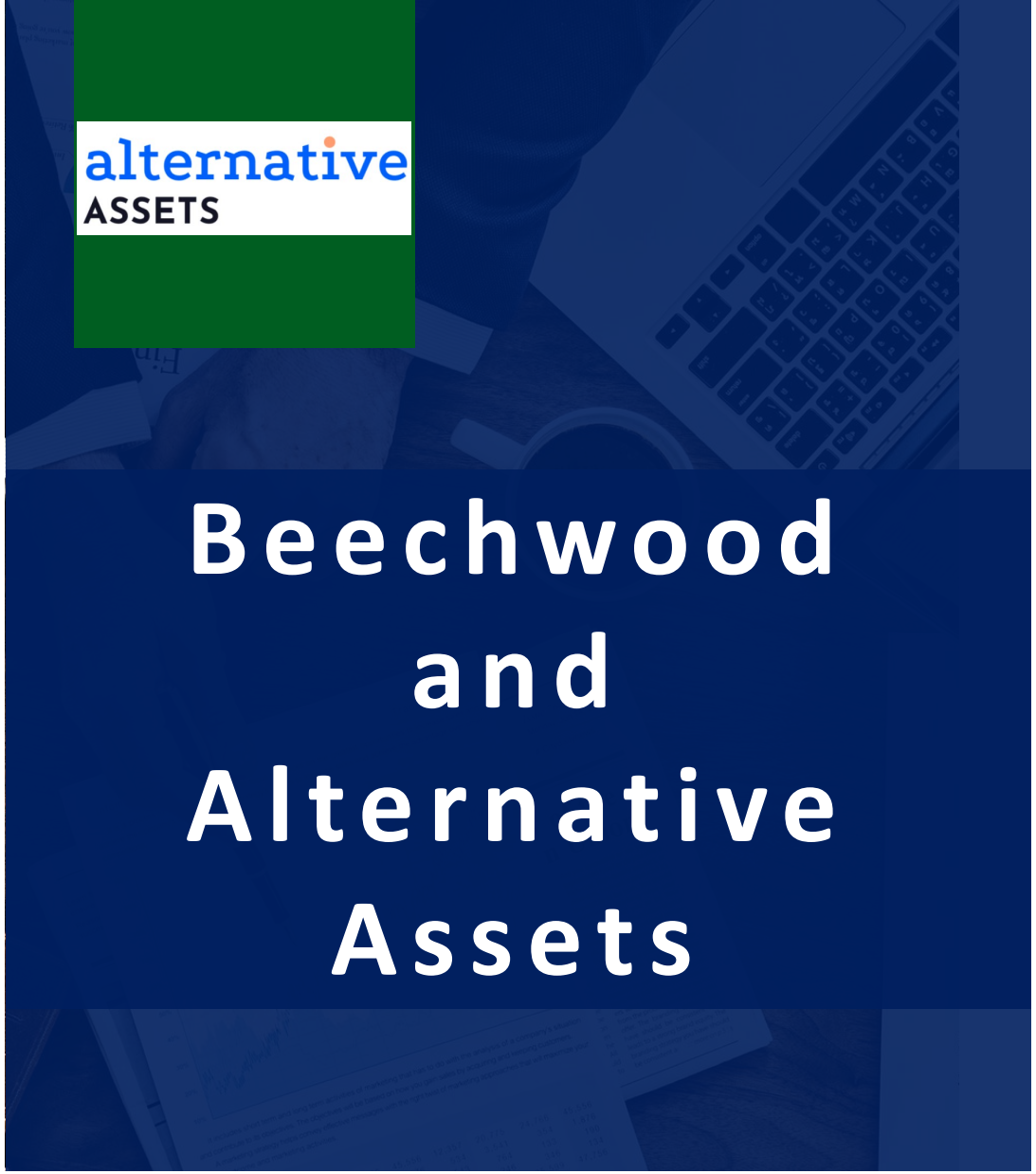
- Founded in 2003 by a team of seasoned investment banking professionals with broad industry and operational experience
- Work directly with “Middle Market” owners and entrepreneurs interested in financing or selling their businesses
- Manage sales of businesses in, or prior to, bankruptcy as a going concern

alternative ASSETS

Beechwood and Alternative Assets

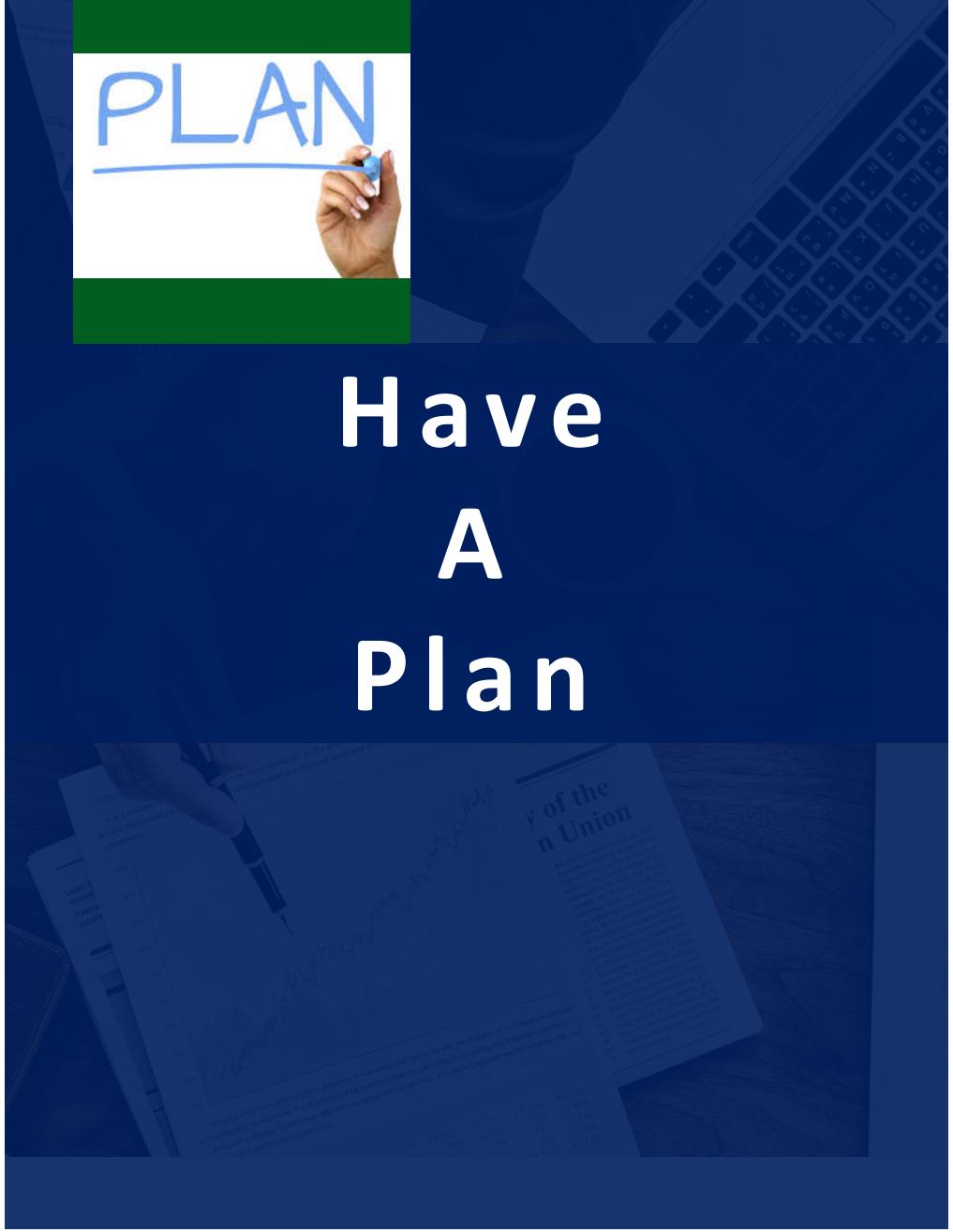
What Happens If.....

- What do you do in the case of crypto currencies in bankruptcy?
  - Identifying relevant assets that can be monetized in bankruptcy
- How do you address treasury management?
  - What about timing?
  - What are the risks during liquidation?
- What are the “tools” available to the Estate’s professionals and representatives when valuing crypto currencies?
- What do you do when you have a business as a going concern that has a non-operating asset like crypto on its balance sheet?



Alternative Assets Crypto & Other

- Strip out Non-Essential operating assets prior to, or concurrent with, sale process:
  - Cryptocurrencies (Bitcoin, Litecoin, Ethereum, etc.)
  - Digital Assets (digital securities and coins)
  - Collectibles (memorabilia)
  - Other
- Act as Crypto/Alternative Asset Banker for Non-Essential Assets
  - More relevant on larger amounts
  - Wholesale approach to lock-in pricing without impacting the market (minimize market impact)
  - Auction-oriented process to maximize value
  - Known network of contacts to quickly access market-makers and key buyers
  - Explore potential borrowing capacity using Crypto or other Non-Essential Assets as collateral



Plan Ahead

Planning is Critical

- Crypto is volatile
- Market swings can be transaction-killers
- Time is not on your side – time can also be a transaction-killer
- Having a Crypto Plan can make all the difference

The Team

Richard Conroy

(Partner)

30+ years in investment and commercial banking and financial consulting. Led and executed numerous complex leveraged transactions.

Co-founded Beechwood's predecessor, The Rockland Group in 2003. Managing Director at Millburn Capital Group and Amper Investment Banking.

Previously at Dresdner Kleinwort Wasserstein as head of the NY Leveraged Finance Group and founded the Real Estate and Public Finance Groups.

Prior to Dresdner, served in various capacities at Fortis Capital, Citibank and PNC.

BS and MBA in accounting from The Kelley School of Business at Indiana University.

Holds licenses with FINRA: Series 7, Series 63, Series 27, Series 79 and Series 24.

Mark Furman

(Partner)

40+ years providing merger and acquisitions and financing services. Joined Beechwood in March 2019.

Founded CVF Securities in 1989, a registered broker-dealer (dba Millburn Capital Group), providing buy and sell-side M&A and financing services to middle market companies (sold in 2017).

Previously a Managing Director in the Media and Telecommunications Investment Banking Group at CIBC Oppenheimer and a VP in the Media Group of Chase Manhattan Bank.

BA from SUNY Binghamton,
MBA from NYU.

Holds licenses with FINRA: Series 7, Series 79, Series 24 and Series 63.

Scott Rothman

(Partner)

20+ years of banking, capital markets and consulting experience. Joined Beechwood in March 2019.

Co-founded JFD Securities in 2002 (sold 2016), a registered broker-dealer providing option trading strategies and derivative execution to global hedge funds, asset managers and mutual funds.

Previously held management, sales and investment positions in several companies in digital assets and blockchain, fintech, healthcare, gaming, foreign exchange and real estate industries.

BA from Penn State,
MBA from Rutgers.

Holds FINRA Licenses: Series 4, Series 7, Series 24, Series 55 and Series 63.

Contact Information

BEECHWOOD CAPITAL ADVISORS

343 Millburn Avenue, Suite 208,
Millburn NJ 07041

973-264-9952

908-845-0263

www.beechwoodcapitaladvisors.com

PARTNERS

Richard Conroy

rconroy@beechwoodcapitaladvisors.com

732-770-5036

Scott Rothman

srothman@beechwoodcapitaladvisors.com

973-985-9533

Mark Furman

mfurman@beechwoodcapitaladvisors.com

973-650-3994

BEECHWOOD
CAPITAL ADVISORS

August 2021

www.beechwoodcapitaladvisors.com

Capital Raising and M&A for the Middle Market

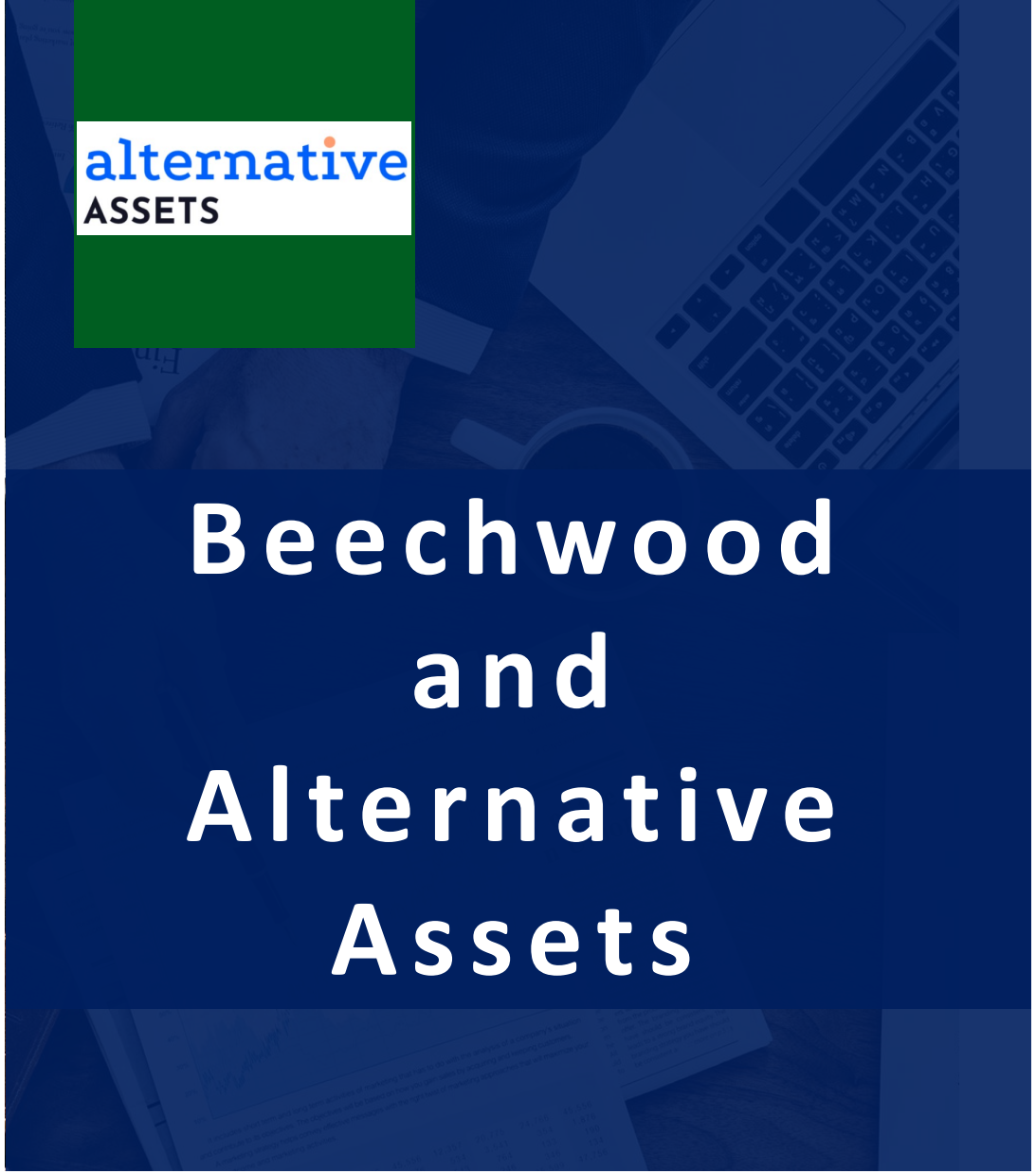
- Founded in 2003 by a team of seasoned investment banking professionals with broad industry and operational experience
- Work directly with “Middle Market” owners and entrepreneurs interested in financing or selling their businesses
- Manage sales of businesses in, or prior to, bankruptcy as a going concern

alternative ASSETS

Beechwood and Alternative Assets

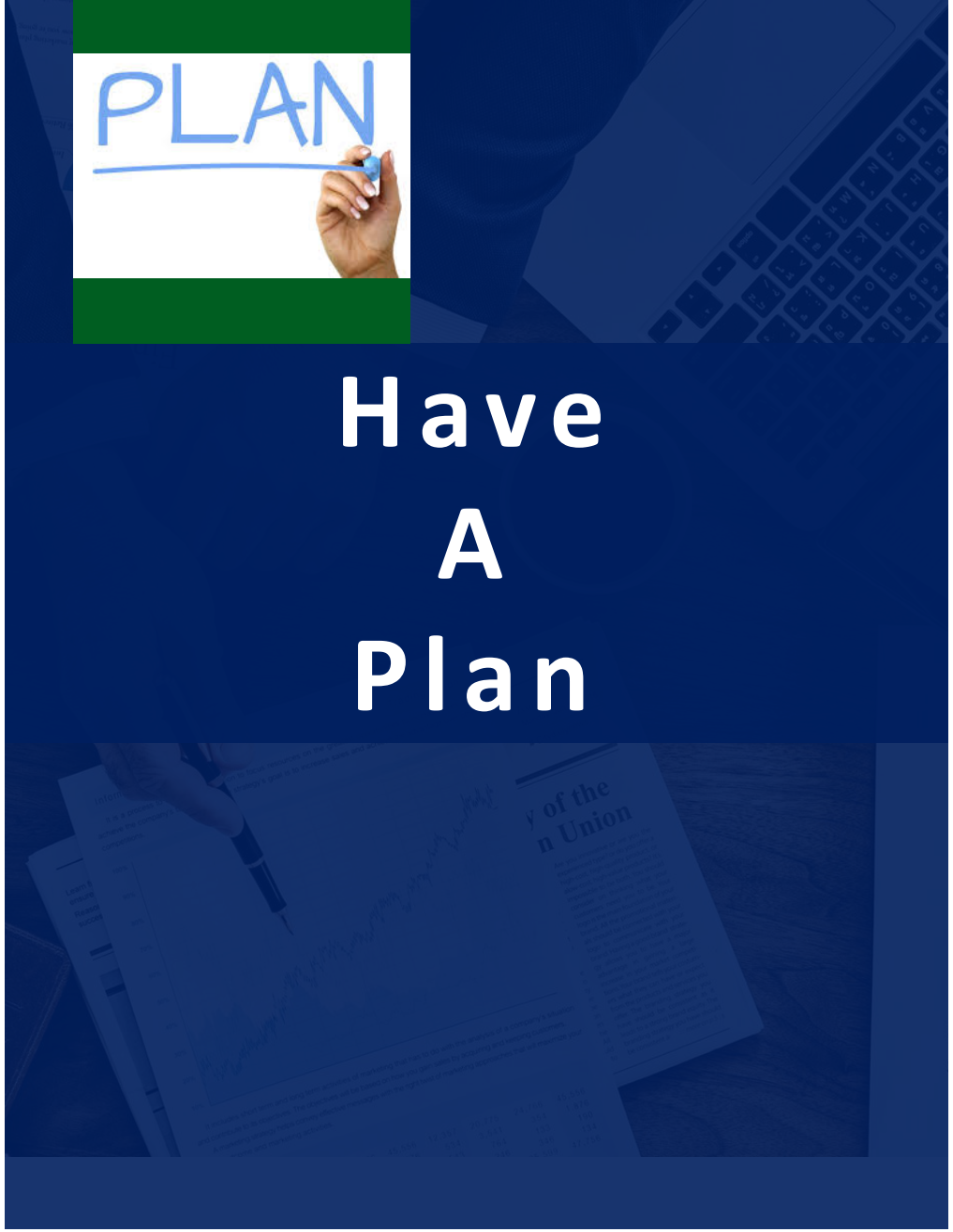
What Happens If.....

- What do you do in the case of crypto currencies in bankruptcy?
  - Identifying relevant assets that can be monetized in bankruptcy
- How do you address treasury management?
  - What about timing?
  - What are the risks during liquidation?
- What are the “tools” available to the Estate’s professionals and representatives when valuing crypto currencies?
- What do you do when you have a business as a going concern that has a non-operating asset like crypto on its balance sheet?



Alternative Assets Crypto & Other

- Strip out Non-Essential operating assets prior to, or concurrent with, sale process:
  - Cryptocurrencies (Bitcoin, Litecoin, Ethereum, etc.)
  - Digital Assets (digital securities and coins)
  - Collectibles (memorabilia)
  - Other
- Act as Crypto/Alternative Asset Banker for Non-Essential Assets
  - More relevant on larger amounts
  - Wholesale approach to lock-in pricing without impacting the market (minimize market impact)
  - Auction-oriented process to maximize value
  - Known network of contacts to quickly access market-makers and key buyers
  - Explore potential borrowing capacity using Crypto or other Non-Essential Assets as collateral



Plan Ahead

Planning is Critical

- Crypto is volatile
- Market swings can be transaction-killers
- Time is not on your side – time can also be a transaction-killer
- Having a Crypto Plan can make all the difference

The Team

Richard Conroy

(Partner)

30+ years in investment and commercial banking and financial consulting. Led and executed numerous complex leveraged transactions.

Co-founded Beechwood's predecessor, The Rockland Group in 2003. Managing Director at Millburn Capital Group and Amper Investment Banking.

Previously at Dresdner Kleinwort Wasserstein as head of the NY Leveraged Finance Group and founded the Real Estate and Public Finance Groups.

Prior to Dresdner, served in various capacities at Fortis Capital, Citibank and PNC.

BS and MBA in accounting from The Kelley School of Business at Indiana University.

Holds licenses with FINRA: Series 7, Series 63, Series 27, Series 79 and Series 24.

Mark Furman

(Partner)

40+ years providing merger and acquisitions and financing services. Joined Beechwood in March 2019.

Founded CVF Securities in 1989, a registered broker-dealer (dba Millburn Capital Group), providing buy and sell-side M&A and financing services to middle market companies (sold in 2017).

Previously a Managing Director in the Media and Telecommunications Investment Banking Group at CIBC Oppenheimer and a VP in the Media Group of Chase Manhattan Bank.

BA from SUNY Binghamton,
MBA from NYU.

Holds licenses with FINRA: Series 7, Series 79, Series 24 and Series 63.

Scott Rothman

(Partner)

20+ years of banking, capital markets and consulting experience. Joined Beechwood in March 2019.

Co-founded JFD Securities in 2002 (sold 2016), a registered broker-dealer providing option trading strategies and derivative execution to global hedge funds, asset managers and mutual funds.

Previously held management, sales and investment positions in several companies in digital assets and blockchain, fintech, healthcare, gaming, foreign exchange and real estate industries.

BA from Penn State,
MBA from Rutgers.

Holds FINRA Licenses: Series 4, Series 7, Series 24, Series 55 and Series 63.

Contact Information

BEECHWOOD CAPITAL ADVISORS

343 Millburn Avenue, Suite 208,
Millburn NJ 07041

973-264-9952

908-845-0263

www.beechwoodcapitaladvisors.com

PARTNERS

Richard Conroy

rconroy@beechwoodcapitaladvisors.com

732-770-5036

Scott Rothman

srothman@beechwoodcapitaladvisors.com

973-985-9533

Mark Furman

mfurman@beechwoodcapitaladvisors.com

973-650-3994

UNITED STATES OF AMERICA
FINANCIAL CRIMES ENFORCEMENT NETWORK
DEPARTMENT OF THE TREASURY

IN THE MATTER OF:	)	
	)	
	)	Number 2020-2
Larry Dean Harmon	)	
d/b/a Helix	)	
	)	
Akron, Ohio	)	

ASSESSMENT OF CIVIL MONEY PENALTY

I. INTRODUCTION

The Financial Crimes Enforcement Network (FinCEN) has determined that grounds exist to assess a civil money penalty against Larry Dean Harmon, as the primary operator of Helix, and as the Chief Executive Officer (CEO) and primary operator of Coin Ninja LLC (Coin Ninja), pursuant to the Bank Secrecy Act (BSA) and regulations issued pursuant to that Act.[1]

FinCEN has the authority to investigate and impose civil money penalties on money services businesses (MSBs) that willfully violate the BSA and on current and former employees who willfully participate in such violations.[2] Rules implementing the BSA state that "[o]verall authority for enforcement and compliance, including coordination and direction of procedures and activities of all other agencies exercising delegated authority under this chapter" has been delegated by the Secretary of the Treasury to FinCEN.[3] At all relevant times, both Mr. Harmon, doing business as Helix, and Coin Ninja were "money transmitters" as defined at 31 C.F.R § 1010.100(ff)(5) and a "financial institutions" as defined at 31 C.F.R § 1010.100(t).

1. The BSA is codified at 12 U.S.C. §§ 1829b, 1951-1959 and 31 U.S.C. §§ 5311-5314, 5316-5332. Regulations implementing the BSA appear at 31 C.F.R. Chapter X.
2. Treasury Order 180-01 (July 1, 2014); 31 U.S.C. § 5321(a); 31 C.F.R. § 1010.810(a).
3. 31 C.F.R. § 1010.810(a).

Mr. Harmon has been indicted in the District of Columbia under related criminal charges pursuant to 18 U.S.C. §§ 1956 and 1960 for conspiracy to launder monetary instruments and the operation of an unlicensed money transmitting business.[4]

II. JURISDICTION

Mr. Harmon, doing business as Helix, operated as an "exchanger" of convertible virtual currencies, accepting bitcoin and transmitting bitcoin to another person or location by a variety of means.[5] Beginning on or about June 6, 2014, through on or about December 16, 2017, Mr. Harmon doing business as Helix, conducted over 1,225,000 transactions for customers and is associated with virtual currency wallet addresses that have sent or received over $311 million. FinCEN has identified at least 356,000 bitcoin transactions through Helix between June 2014 and December 2017. Beginning on or about July 13, 2017 through the present, Mr. Harmon served as CEO of Coin Ninja, a Delaware-incorporated and Ohio-located money transmitter that operates as an exchanger of convertible virtual currencies. Mr. Harmon willfully participated in the direction and supervision of Coin Ninja's operations and finances. Exchangers of convertible virtual currency are "money transmitters" as defined at 31 C.F.R § 1010.100(ff)(5) and "financial institutions" as defined at 31 C.F.R § 1010.100(t).

III. DETERMINATIONS

FinCEN has determined that, from on or about June 6, 2014 through December 3, 2019, Mr. Harmon, doing business as Helix, willfully violated the BSA's registration, program, and reporting requirements.[6] Mr. Harmon, doing business as Helix, willfully (a) failed to register as a money services business;[7] (b) failed to implement and maintain an effective anti-money laundering (AML) program; [8] and (c) failed to report certain

4. *United States of America v. Larry Dean Harmon*, 19-cr-00395, (D.C. DC, Dec. 3, 2019).
5. FIN-2013-G001, "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies," March 18, 2013.
6. In civil enforcement of the BSA under 31 U.S.C. §5321(a)(1), to establish that a financial institution or individual acted willfully, the government need only show that the financial institution or individual acted with either reckless disregard or willful blindness. The government need not show that the entity or individual had knowledge that the conduct violated the BSA, or that the entity or individual otherwise acted with an improper motive or bad purpose.
7. 31 U.S.C. § 5330 and 31 C.F.R. § 1022.380.
8. 31 U.S.C. § 5318(h) and 31 C.F.R. § 1022.210.

suspicious activity.[9] In addition, FinCEN has determined that on or about July 13, 2017 through December 3, 2019, Mr. Harmon willfully participated in Coin Ninja's failure to register as a money services business.[10]

These violations, and the governing facts and law surrounding the violations, are described more fully in the Statement of Facts (Attachment A), which is fully incorporated here by reference.

IV. CIVIL MONEY PENALTY

FinCEN determined that Mr. Harmon, in his roles with Helix and Coin Ninja, willfully violated the BSA and its implementing regulations, as described in this ASSESSMENT and Attachment A, and that grounds exist to assess a civil money penalty for these violations.[11] FinCEN determined that the maximum penalty in this matter is **$209,144,554**.[12]

FinCEN may impose a civil money penalty of $57,317 for each willful violation of AML program requirements assessed on or after October 10, 2019.[13] The BSA states that a "separate violation" of the requirement to establish and implement an effective AML program occurs "for each day that the violation continues."[14] The authorized penalty for each violation of MSB registration requirements assessed on or after October 10, 2019 is $8,457.[15] The BSA states that "each day" a violation of the failure to register as a MSB continues "constitutes a separate violation."[16] FinCEN may impose a penalty not to exceed the greater of the amount involved in the transaction (but capped at $229,269) or $57,317 for each willful violation of SAR requirements assessed on or after October 10, 2019.[17]

---

9. 31 U.S.C. § 5318(g)(1) and 31 C.F.R. § 1022.320.
10. 31 U.S.C. § 5330 and 31 C.F.R. § 1022.380.
11. 31 U.S.C. §§ 5321 and 5330(e); 31 C.F.R. §§ 1010.820 and 821.
12. Pursuant to the Federal Civil Penalties Inflation Act of 2015 (Pub. L. 114-74) ("the 2015 Act"), increased civil money penalties apply only with respect to underlying violations occurring after the enactment of the 2015 Act, i.e., after November 2, 2015.
13. 31 U.S.C. § 5321(a)(1); 31 C.F.R. §§ 1010.820(i) and 821.
14. 31 U.S.C. § 5321(a)(1).
15. 31 U.S.C. § 5330(e)(1); 31 C.F.R. §§ 1022.380(e) and 1010.821.
16. 31 U.S.C. § 5330 and 31 C.F.R. § 1022.380(e).
17. 31 U.S.C. § 5321(a)(1); 31 C.F.R. §§ 1010.820(i) and 821.

V. CONSIDERATION OF PENALTY FACTORS

On February 6, 2020, FinCEN provided Helix with a written pre-assessment notice that included a draft ASSESSMENT and Statement of Facts (the "PAN package"). The PAN package provided Helix with FinCEN's charges outlining violations of the BSA and its implementing regulations, the factors taken into consideration in determining whether to assess a civil money penalty and the proposed civil money penalty amount, and instructions on how to respond to these charges. Helix responded, through counsel, on March 6, 2020 denying that it operated as a MSB and requesting more time to respond to FinCEN's Statement of Facts. FinCEN provided Helix with multiple opportunities to respond to the PAN package. To date, over eight months since FinCEN issued its PAN package, Helix has not provided any additional information or documentation responding to the allegations or considerations contained in FinCEN's PAN package. As such, FinCEN concludes that Helix has decided not to submit any new facts or explanations for consideration. In light of this, FinCEN has considered the following factors in determining the disposition of this matter:

1. Nature and seriousness of the violations and harm to the public. The violations outlined in this ASSESSMENT are considered by FinCEN to be of a serious and egregious nature. The BSA and its implementing regulations require MSBs and money transmitters such as Helix to develop and implement a risk-based AML program designed to deter illicit financial activity and report suspicious activity, among other things, in order to assist law enforcement in detecting crimes. In this instance, Helix operated as a MSB in a high-risk industry that deals in convertible virtual currencies without developing an AML program and, in fact, provided its services in such a manner that it assisted and facilitated illicit financial activity. As a sophisticated enterprise, Helix worked in conjunction with darknet marketplaces to launder illicit bitcoin proceeds and actively marketed its services as an anonymity-enhancing service to launder bitcoin from illicit activity. For example, FinCEN observed bitcoin transactions equal to $121,511,877 transferred to darknet-associated addresses by, through, or to Helix.

2. Impact of violations on FinCEN's mission to safeguard the financial system. Helix was totally and completely deficient in its compliance with the BSA and its implementing regulations during the entire course of Helix's operation. FinCEN analysis evidenced that Helix failed to maintain all required elements of an AML program. During the lifespan of the MSB, Helix developed no AML program and was vulnerable to illicit use. In addition to having no AML program, Helix further failed to designate a compliance officer, conduct any AML training for employees, and never conducted an independent test required under law. Rather than collect customer data as part of a viable AML program, Helix asserted that it deleted even the minimal customer information it did collect for all transactions it facilitated. Helix also failed to conduct appropriate suspicious activity monitoring from 2014 through 2017, making it difficult to completely ascertain the number of specific reporting violations that exist. Independent FinCEN analysis of Helix's public records and analysis of convertible virtual currency blockchains identified at least 245,817 instances in which suspicious transactions took place. Yet, Helix failed to file a single SAR throughout the corresponding time period.

3. Pervasiveness of wrongdoing within the financial institution. Helix openly flaunted existing regulatory requirements and went out its way to create ways for darknet customers and vendors to avoid law enforcement detection. Helix purposefully created a system to facilitate illicit activity, which was recognized by darknet drug vendors like AlphaBay – a marketplace that integrated Helix into its platform. Rather than institute policies and procedures to comply with the BSA, Helix instead instituted policies and procedures that allowed customers of darknet marketplaces to launder bitcoin through Helix.

4. History and duration of violations. Helix operated for over three years, from April 2014 to December 2017, without appropriate AML policies and procedures in place. Helix did not implement even basic AML program requirements and specifically sought to launder bitcoin from illegal activity.

5. Failure to terminate the violations. After Helix closed operations in December 2017, Helix continued to operate another unregistered MSB by creating, controlling, and operating the money transmitter Coin Ninja LLC in 2017, which operated through February 6, 2020.

6. Financial gain or other benefit as a result of violation. Helix made a significant financial gain in administrator fees from its facilitation of transactions with darknet marketplaces, ransomware, child exploitation websites, and unregistered MSBs. Helix did not expend any resources on compliance with the BSA and its implementing regulations.

7. Cooperation. Helix agreed to two statute of limitations tolling agreements with FinCEN.

8. Systemic nature of violations. Helix's systemic failure to report potentially suspicious activity led to shortcomings that denied potentially critical information to the BSA database for at least a three-year period. FinCEN's independent investigation found that Helix conducted numerous potentially suspicious transactions with darknet marketplaces, ransomware, unregistered MSBs, and other mixing platforms offering similar money laundering services.

9. Timely and Voluntary Disclosure of Violations. FinCEN did not consider this as an aggravating or mitigating factor in this matter.

10. Penalties by Other Government Entities. FinCEN is the sole government regulator with authority to pursue civil violations of the BSA and its implementing regulations for MSBs.[18] FinCEN has considered Helix's indictment in the District of Columbia under 18 U.S.C. § § 1956 and 1960 for conspiracy to launder monetary instruments and the operation of an unlicensed money transmitting business.[19]

18. 31 C.F.R. § 1010.810(a); Treasury Order 180-01 (July 1, 2014).
19. *United States of America v. Larry Dean Harmon*, 19-cr-00395, (D.C. DC, Dec. 3, 2019).

As a result of the analysis described above, FinCEN hereby imposes a penalty in the amount of **$60,000,000**.

Kenneth A. Blanco Date:
Director
Financial Crimes Enforcement Network
U.S. Department of the Treasury

Attachment A

Statement of Facts

I. Background

A. Larry Dean Harmon and Coin Ninja

1. Larry Dean Harmon (Mr. Harmon) is a U.S. person residing in Akron, Ohio. Mr. Harmon was the creator, administrator, and primary operator of Grams, a darknet website that operated on the onion router (Tor) network and advertised itself as the "Google of the Darkweb" from in or about April 2014 through on or about December 16, 2017. Grams served as a search engine and content aggregator allowing users to search for illicit goods sold on darknet markets. Grams also indexed darknet .onion pages for vendors of illicit goods such as narcotics, illegal firearms, and stolen Personally Identifiable Information (PII).

2. On or about June 2014, Mr. Harmon began operating and administrating a convertible virtual currency exchanger called Helix through the Grams darknet .onion site.[1] Mr. Harmon was the primary administrator and operator of Helix. Helix was a service linked to and affiliated with Grams, and the two services were sometimes referred to collectively as "Grams-Helix." Helix operated what is commonly referred to as a "mixer" or "tumbler" of the convertible virtual currency bitcoin – charging customers a fee to send bitcoin to a designated address in a manner designed to conceal and obfuscate the source or owner of the bitcoin. Mr. Harmon offered customers two options to transmit "tumbled" bitcoin: Helix and Helix Light. Helix was built as a function into customer's Grams "account" and operated in the following manner:

   a. Customers would send bitcoin to a wallet associated with their Grams account;
   b. Customers would then complete a Helix withdrawal form, which included the amount to withdraw, a destination address, and the ability to set a time delay for the transactions;
   c. Helix would transmit the bitcoin deposited into their wallet to one of numerous accounts held at different exchangers of convertible virtual currency;
   d. Helix would take bitcoin from a different account it held and transmit that bitcoin to a different bitcoin address;
   e. From this bitcoin address, Helix would then transmit bitcoin to the customer, minus a fee, into the previously provided customer destination address;
   f. Helix asserted that it deleted customer information after seven days, or allowed customers to delete their logs manually after a withdrawal.

1. "Introducing Grams Helix: Bitcoin Cleaner," DeepDotWeb, June 22, 2014, Accessed January 24, 2018.

3. Helix Light was a service of Helix that allowed individuals to transact without creating a Grams "account." Helix Light conducted transactions in the following manner:

   a. Customers were asked to provide a destination address to receive bitcoins;
   b. Helix Light would provide an address to which the customer would send the desired amount of bitcoin between .02 and 6 bitcoins;
   c. Helix Light would transmit the bitcoin deposited into their wallet to one of numerous accounts held at different exchangers of convertible virtual currency;
   d. Helix Light would take bitcoin from a different account it held and transmit that bitcoin to a different bitcoin address;
   e. From this bitcoin address, Helix Light would then transmit bitcoin to the customer, minus a fee, into the previously provided customer destination address;

4. On or about July 13, 2017, Mr. Harmon, through his legal representative, registered Coin Ninja LLC (Coin Ninja) in Delaware. Mr. Harmon later filed a corporate registration in Ohio on November 8, 2017.[2] Mr. Harmon is the Chief Executive Officer of Coin Ninja, which operates as a money services business. Mr. Harmon willfully participated in the direction and supervision of Coin Ninja's operations and finances. Coin Ninja has stated on its Frequently Asked Questions (FAQ) page that it also provided a "mixing" service including an "FAQ" titled "Why should I mix my bitcoins?"[3] Coin Ninja offers a service called DropBit, which describes itself as "like Venmo for Bitcoin" allowing customers to accept and transmit bitcoin through text messages or Twitter handles.[4] Mr. Harmon has advertised Coin Ninja's DropBit service on Reddit, under the moniker "doolbman," as a service that helps circumvent know your customer procedures.[5]

B. The Financial Crimes Enforcement Network

5. The Financial Crimes Enforcement Network (FinCEN) is a bureau within the Department of Treasury. Pursuant to 31 C.F.R. § 1010.810, FinCEN has "[o]verall authority for enforcement and compliance, including coordination and direction of procedures and activities of all other agencies exercising delegated authority" under the Bank Secrecy Act (BSA) and its implementing regulations. FinCEN regulates money services businesses and other financial institutions under the BSA.[6]

2. Registration of Foreign for Profit Limited Liability Company Document Number 201731201776, State of Ohio Secretary of State, November 8, 2017.
3. "Frequently Asked Questions," https://coinninja.io/faq, February 14, 2018.
4. @dropbitapp, Twitter, https://twitter.com/dropbitapp, accessed November 20, 2019.
5. doolbman, "Send Bitcoin instead of Venmo or PayPal. Spread the wealth," https://www.reddit.com/r/Bitcoin/comments/awnvoi/send_bitcoin_instead_of_venmo_or_paypal_spread/ehnv18u/?context=3, March 2, 2019.
6. *See* Treasury Order 180-01 (July 1, 2014).

C. Mixers and Tumblers Status as Money Transmitters Under the BSA

6. Providers of anonymizing services, commonly referred to as "mixers" or "tumblers," are either persons that accept convertible virtual currencies and retransmit them in a manner designed to prevent others from tracing the transmission back to its source (anonymizing services provider). An anonymizing services provider is a money transmitter under FinCEN regulations because it accepts and transmits convertible virtual currencies.[7]

II. Anti-Money Laundering/Bank Secrecy Act Violations

A. Failure to Register as a Money Services Business

7. The BSA and its implementing regulations require the registration of an MSB within 180 days of beginning operations and the renewal of such registration every two years.[8]

8. Mr. Harmon began operating Helix in June 2014 and ceased operations in December 2017 and never registered as an MSB with FinCEN.

9. Before closing Helix, Mr. Harmon began operating Coin Ninja on or about July 13, 2017. Neither Coin Ninja, nor its DropBit service, have ever registered as an MSB with FinCEN.

B. Failure to Implement an Anti-Money Laundering Program

10. Since July 24, 2002, MSBs have been required to "develop, implement, and maintain an effective anti-money laundering (AML) program."[9] The program must be in writing and commensurate with the risks posed by the location and size of, and the nature and volume of the financial services provided by the MSB.[10] An effective AML program is one that is reasonably designed to prevent the MSB from being used to facilitate money laundering and the financing of terrorist activities.[11] MSBs must, "[i]ncorporate policies, procedures, and internal controls reasonably designed to assure compliance…."[12] An MSB is also required to designate a person to assure day to day compliance with its AML program.[13] An MSB must provide for training of personnel, including training in the detection of suspicious transactions and provide for independent review to monitor and maintain an adequate program.[14] Mr. Harmon never implemented any type of AML program related to Helix and failed to comply with all of the aforementioned requirements.

---

7. "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies," (FIN-2019-G001)," May 9, 2019, p.19-20.
8. 31 U.S.C. § 5330 and 31 C.F.R. §§ 1022.380(b)(2) and (3).
9. 31 C.F.R. § 1022.210(a).
10. 31 C.F.R. § 1022.210(b).
11. 31 C.F.R. § 1022.210(a).
12. 31 C.F.R. § 1022.210(d)(1).
13. 31 C.F.R. § 1022.210(d)(2).
14. 31 C.F.R. § 1022.210(d)(3)-(4).

i. Policies, Procedures, and Internal Controls

11. An MSB is required to have a compliance program that includes "[a] system of internal controls to assure ongoing compliance."[15] Mr. Harmon failed to establish and maintain appropriate internal controls to ensure compliance with the BSA's reporting requirements during the operation of his business. In fact, Mr. Harmon actively aided cybercriminals and other threat actors in circumventing the policies, procedures, and internal controls in place at U.S.-based convertible virtual currency exchanges. Through his services Mr. Harmon promoted unlawful online activities by concealing the nature, the location, the source, the ownership, and the control of the proceeds of online drug sales, amongst other illegal online activities.

12. Mr. Harmon publicly advertised Helix on Reddit forums dedicated to darknet marketplaces, actively seeking out and facilitating high-risk transactions directly through customer service and feedback. On December 7, 2014, Mr. Harmon, using the online moniker "gramsadmin," posted, "Helix does exactly what it says it does, breaks the blockchain taint so a transaction can't be followed through the blockchain. Helix gives you new bitcoins [sic] from a different pool, that have never been on the darkweb."[16] On November 24, 2014, Mr. Harmon, using the same online moniker and forum, identified transactions passing from a specific darknet marketplace through Helix, stating "Since Helix uses expiring addresses and all the Agora withdrawals just started coming[.] I have a bunch of unclaimed bitcoins."[17]

13. Despite requiring account creation for transactions through Helix, Mr. Harmon chose not to collect information on any of the over 809,500 unique addresses sending and receiving bitcoin. In addition, Mr. Harmon developed Helix Light so that customers could conduct transactions without even creating the accounts required by the Helix service offered through his Grams platform. As a result, Mr. Harmon failed to collect and verify customer names, addresses, or any other related customer identifiers on over 1.2 million transactions between June 2016 and December 2017 alone.

14. In fact, during its entire operational period, Mr. Harmon openly advertised Helix as a service that did not conduct customer due diligence, stating "My goals with Helix light [and] Regular helix [have] always and will always work to perfection for tumbling bitcoins and keeping a user anonymous."[18] During the operational period, Mr. Harmon conducted over $311 million worth of transactions in convertible virtual currencies without performing appropriate due diligence on transactions or customers.

---

15. 31 C.F.R. § 1022.210(b)(2)(i).
16. gramsadmin, "Helix : Agora bitcoin claim process?," https://www.reddit.com/r/ DarkNetMarkets/comments/2oi5jh/ helix_deanonymization_the_response/, December 7, 2014.
gramsadmin, "Helix : Agora bitcoin claim process?,"
17. gramsadmin, "Helix : Agora bitcoin claim process?," https://www.reddit.com/r/DarkNetMarkets/comments/2nanzl/ helix_agora_bitcoin_claim_process/Reddit, November 24, 2014.
18. gramsadmin, "Helix : Agora bitcoin claim process?," https://www.reddit.com/r/DarkNetMarkets/comments/2nanzl/ helix_agora_bitcoin_claim_process/Reddit, November 24, 2014.

15. Mr. Harmon also failed to implement policies and procedures to file reports required by the BSA and to create and retain appropriate records.[19] In public fora, Mr. Harmon advertised that "All logs are deleted after 7 days, but you can deleted the logs off the server manually after the helix withdraw is complete."[20] Mr. Harmon asserted that he deleted any customer information Helix had after a period of seven days.[21] Mr. Harmon also claimed to allow customers to delete their own customer information at will. Such a policy made it impossible for Mr. Harmon to comply with the requirements of the BSA. During its operations over 1.2 million transactions passed through Helix.

16. More specifically, Mr. Harmon failed to implement appropriate policies, procedures, and internal controls to detect and report potentially suspicious transactions. FinCEN identified a significant volume of transactions that bore indicia of money laundering and other illicit activity. These included transactions supporting illegal narcotics and controlled substances, drug paraphernalia, counterfeit and fraud-related goods and services, child exploitation websites, and white nationalist/neo-Nazi groups. As detailed in Section II. C (below), potentially suspicious activity going through sites controlled and operated by Mr. Harmon totaled over $121 million.

17. Mr. Harmon failed to mitigate risks associated with Tor-enabled browsers. While use of Tor in and of itself is not suspicious, the many transactions that take place through an anonymizing internet browser, such as darknet marketplaces, may be a strong indicator of potential illicit activity when no additional due diligence is conducted. Because of this, Mr. Harmon failed to determine customer identity and whether or not the funds were derived from illegal activity.

18. Mr. Harmon failed to apply due diligence measures proportionate to the risks arising to any jurisdictions with AML/CFT deficiencies.[22] These deficiencies were exacerbated by Mr. Harmon's failure to implement appropriate due diligence over transactions occurring through Tor-enabled browsers. For example, according to FinCEN's analysis, from June 2014 through December 2017 Mr. Harmon accepted and processed multiple transactions with Iran-affiliated accounts. Mr. Harmon failed to implement policies, procedures, and internal controls to review for potential suspicious activity occurring by, through, or to jurisdictions with a heightened risk for money laundering and terrorist finance.

19. 31 C.F.R. § 1022.210(d)(1)(i)(B) and (C).
20. gramsadmin, "New Grams' Helix," https://www.reddit.com/r/onions/comments/28t66t/new_grams_helix/, June 22, 2014.
21. Introducing Grams Helix: Bitcoins Cleaner, DeepDotWeb, June 22, 2014.
22. *See* "Advisory on the Financial Action Task Force-Identified Jurisdictions with AML/CFT Deficiencies (FIN-2015-A002)," July 17, 2015; "Advisory on the Financial Action Task Force-Identified Jurisdictions with AML/CFT Deficiencies (FIN-2016-A001)," January 19, 2016.

ii. Compliance Officer

19. An MSB is also required to designate a person to assure day to day compliance with their compliance program and the BSA. This person is responsible for assuring that the MSB files reports, and creates and retains records, that the compliance program is updated as necessary to reflect the current requirements of the BSA, and provides appropriate training.[23] At no point in its operations did Mr. Harmon designate a person to assure day to day compliance with their compliance program and the BSA.

iii. Training

20. An MSB must provide for training of personnel, including training in the detection of suspicious transactions.[24] Mr. Harmon failed to train appropriate personnel in BSA recordkeeping and reporting requirements and failed to train personnel in identifying, monitoring, and reporting suspicious activity.

iv. Independent Testing

21. An MSB must provide for independent review to monitor and maintain an adequate program.[25] At no point in its operations did Mr. Harmon conduct an independent test.

C. Failure to File Suspicious Activity Reports

22. The BSA and its implementing regulations require an MSB to report a transaction that the MSB "knows, suspects, or has reason to suspect" is suspicious, if the transaction is conducted or attempted by, at, or through the MSB, and the transaction involves or aggregates to at least $2,000 in funds or other assets.[26] A transaction is "suspicious" if the transaction: (a) involves funds derived from illegal activity; (b) is intended or conducted in order to hide or disguise funds or assets derived from illegal activity, or to disguise the ownership, nature, source, location, or control of funds or assets derived from illegal activity; (c) is designed, whether through structuring or other means, to evade any requirement in the BSA or its implementing regulations; (d) has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the casino knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction; or (e) involves use of the MSB to facilitate criminal activity. An MSB must file a SAR no later than 30 calendar days after initially detecting facts that may constitute a basis for filing a suspicious activity report.[27]

23. 31 C.F.R. § 1022.210(d)(2)(i)-(iii).
24. 31 C.F.R. § 1022.210(d)(3).
25. 31 C.F.R. § 1022.210(d)(4).
26. 31 C.F.R. § 1022.320.
27. 31 C.F.R. §§ 1022.320(a)(2)(i) – (iv).

23. FinCEN has identified at least 2,464 instances in which Mr. Harmon failed to file a SAR for transactions involving Helix.

i. Darknet and other Illicit Markets

24. Helix addresses were found to interact directly with 39 darknet marketplaces and other illicit markets where individuals bought and sold illicit goods and services. Bitcoin is the most common medium of exchange on these marketplaces. FinCEN observed 241,594 direct bitcoin transactions worth $39,074,476.47 with darknet and other illicit marketplace-associated addresses, not including indirect transactions. At least 2,097 of these direct transactions were for an amount over $2,000. Mr. Harmon failed to file a SAR on all darknet and other illicit market transactions.

25. **Abraxas Market.** Abraxas Market was a Tor-network based darknet market in operation from in and around December 2014 to around November 2015 that sold illegal narcotics and controlled substances, drug paraphernalia, counterfeit and fraud-related goods and services, and other illegal contraband. FinCEN observed Helix conducting 776 bitcoin transactions worth $308,077.74 directly with the Abraxas darknet marketplace. At least 25 of these direct transactions were for an amount over $2,000. Mr. Harmon failed to file a SAR on these transactions.

26. **Agora Market.** Agora Market was a Tor-network based darknet market in operation from in and around January 2014 to around August 2015 that sold illegal narcotics and controlled substances, drug paraphernalia, counterfeit and fraud-related goods and services, and other illegal contraband. FinCEN observed Helix conducting 3,978 bitcoin transactions worth $1,725,338.13 directly with the Agora darknet marketplace. At least 131 of these direct transactions were for an amount over $2,000. Mr. Harmon failed to file a SAR on these transactions.

27. **AlphaBay Market.** AlphaBay Market was a Tor-network based darknet market in operation from in and around December 2014 to July 2017, when the site was seized by law enforcement.[28] At the time of the seizure, AlphaBay was the largest Darknet marketplace in operation, offering a platform for customers to purchase a variety of illegal drugs, guns, and other illegal goods. In or about November 2016, the AlphaBay website recommended to its customers that they use a bitcoin tumbler service to "erase any trace of [their] coins coming from AlphaBay,'' and provided an embedded link to the Tor website for Helix. FinCEN observed Helix conducting 191,988 bitcoin transactions worth $27,066,798 directly with the AlphaBay darknet marketplace. At least 1,201 of these direct transactions were for an amount over $2,000. Mr. Harmon failed to file a SAR on these transactions.

28. "AlphaBay, the Largest Online 'Dark Market,' Shut Down," U.S. Department of Justice, https://www.justice.gov/opa/pr/alphabay-largest-online-dark-market-shut-down, July 20, 2017.

28. **Aviato Market.** Aviato Market was a Tor-network based darknet market in operation from in and around April 2016 to around December 2017 that sold illegal narcotics and controlled substances, drug paraphernalia, counterfeit and fraud-related goods and services, and other illegal contraband. FinCEN observed Helix conducting 406 bitcoin transactions worth $32,439 directly with the Aviato darknet marketplace. Mr. Harmon failed to file a SAR on these transactions.

29. **Black Bank Market.** Black Bank Market was a Tor-network based darknet market in operation from in and around March 2015 to around June 2015 that sold illegal narcotics and controlled substances, drug paraphernalia, counterfeit and fraud-related goods and services, and other illegal contraband. FinCEN observed Helix conducting 453 bitcoin transactions worth $179,681 directly with the Black Bank darknet marketplace. At least nine of these direct transactions were for an amount over $2,000. Mr. Harmon failed to file a SAR on these transactions.

30. **Doctor D Market.** Doctor D Market was a Tor-network based darknet market in operation from in and around March 2015 to around August 2016 that sold illegal narcotics and controlled substances, drug paraphernalia, counterfeit and fraud-related goods and services, and other illegal contraband. FinCEN observed Helix conducting 101 bitcoin transactions worth $43,945 directly with the Doctor D darknet marketplace. At least two of these direct transactions were for an amount over $2,000. Mr. Harmon failed to file a SAR on these transactions.

31. **Dream Market.** Dream Market was a Tor-network based darknet market in operation from in and around November 2013 to April 2019 that sold illegal narcotics and controlled substances, drug paraphernalia, counterfeit and fraud-related goods and services, and other illegal contraband. FinCEN observed Helix conducting 20,724 bitcoin transactions worth $3,544,497 directly with the Dream darknet marketplace. At least 250 of these direct transactions were for an amount over $2,000. Mr. Harmon failed to file a SAR on these transactions.

32. **DutchDrugz Market.** DutchDrugz Market was a Tor-network based darknet market in operation from in and around January 2017 to around January 2018 that sold illegal narcotics and controlled substances, and drug paraphernalia. FinCEN observed Helix conducting 19 bitcoin transactions worth $29,366 directly with the DutchDrugz darknet marketplace. At least five of these direct transactions were for an amount over $2,000. Mr. Harmon failed to file a SAR on these transactions.

33. **Evolution Market.** Evolution Market was a Tor-network based darknet market in operation from in and around January 2014 to around March 2015 that sold illegal narcotics and controlled substances, drug paraphernalia, counterfeit and fraud-related goods and services, and other illegal contraband. FinCEN observed Helix conducting 295 bitcoin transactions worth $114,670 directly with the Evolution darknet marketplace. At least nine of these direct transactions were for an amount over $2,000. Mr. Harmon failed to file a SAR on these transactions.

34. **Flugsvamp Market 2.0.** Flugsvamp Market 2.0 was a Tor-network based darknet market in operation from in and around April 2015 to around September 2018 that sold illegal narcotics and controlled substances, drug paraphernalia, counterfeit and fraud-related goods and services, and other illegal contraband. FinCEN observed Helix conducting 758 bitcoin transactions worth $161,774 directly with the darknet marketplace. At least 22 of these direct transactions were for an amount over $2,000. Mr. Harmon failed to file a SAR on these transactions

35. **Hansa Market.** Hansa Market was a Tor-network based darknet market in operation from in and around August 2015 to around July 2017 that sold illegal narcotics and controlled substances, drug paraphernalia, counterfeit and fraud-related goods and services, and other illegal contraband. Dutch and US law enforcement seized the market and arrested the site owners in 2017.[29] FinCEN observed Helix conducting 4,885 bitcoin transactions worth $635,685 directly with the darknet marketplace. At least 26 of these direct transactions were for an amount over $2,000. Mr. Harmon failed to file a SAR on these transactions.

36. **Hydra Market.** Hydra Market was a Tor-network based darknet market in operation since at least 2014 that sells illegal narcotics and controlled substances, drug paraphernalia, counterfeit and fraud-related goods and services, and other illegal contraband. FinCEN observed Helix conducting 297 bitcoin transactions worth $77,983 directly with the darknet marketplace. At least seven of these direct transactions were for an amount over $2,000. Mr. Harmon failed to file a SAR on these transactions.

37. **Joker's Stash Market.** Joker's Stash Market was an illicit market in operation from in and around October 2014 to around July 2017 that sold stolen credit card numbers and fraud-related goods and services. FinCEN observed Helix conducting 33 bitcoin transactions worth $2,279 directly with the marketplace. Mr. Harmon failed to file a SAR on these transactions.

38. **Middle Earth Marketplace.** Middle Earth Marketplace was a Tor-network based darknet market in operation from in and around July 2014 to in and around November 2015 that sold illegal narcotics and controlled substances, drug paraphernalia, counterfeit and fraud-related goods and services, and other illegal contraband. FinCEN observed Helix conducting 353 bitcoin transactions worth $105,231 directly with the darknet marketplace. At least 11 of these direct transactions were for an amount over $2,000. Mr. Harmon failed to file a SAR on these transactions.

29. "Massive Blow to Criminal Dark Web Activities after Globally Coordinated Operation," Europol, July 20, 2017, https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation.

39. **Nucleus Market.** Nucleus Market was a Tor-network based darknet market in operation from in and around November 2014 to in and around April 2016 that sold illegal narcotics and controlled substances, drug paraphernalia, counterfeit and fraud-related goods and services, and other illegal contraband. FinCEN observed Helix conducting 6,405 bitcoin transactions worth $3,480,201 directly with the darknet marketplace. At least 306 of these direct transactions were for an amount over $2,000. Mr. Harmon failed to file a SAR on these transactions.

40. **Oasis Market.** Oasis Market was a Tor-network based darknet market in operation from in and around March 2016 to around September 2016 that sold illegal narcotics and controlled substances, drug paraphernalia, counterfeit and fraud-related goods and services, and other illegal contraband. FinCEN observed Helix conducting 452 bitcoin transactions worth $102,481 directly with the darknet marketplace. At least 12 of these direct transactions were for an amount over $2,000. Mr. Harmon failed to file a SAR on these transactions.

41. **Russian Anonymous Marketplace.** Russian Anonymous Marketplace (RAMP) was a Tor-network based darknet market in operation from in and around November 2014 to around July 2017 that sold illegal narcotics and controlled substances, drug paraphernalia, counterfeit and fraud-related goods and services, and other illegal contraband. FinCEN observed Helix conducting 256 bitcoin transactions worth $120,047 directly with the darknet marketplace. At least 19 of these direct transactions were for an amount over $2,000. Mr. Harmon failed to file a SAR on these transactions.

42. **Silk Road 2 Market.** Silk Road 2 Market was a Tor-network based darknet market in operation from in and around November 2013 to around November 2014 that sold illegal narcotics and controlled substances, drug paraphernalia, counterfeit and fraud-related goods and services, and other illegal contraband. US law enforcement shutdown the market and arrested the site owner on November 6, 2014.[30] FinCEN observed Helix conducting 17 bitcoin transactions worth $5,881 directly with the darknet marketplace. Mr. Harmon failed to file a SAR on these transactions.

43. **TradeRoute Market.** TradeRoute Market was a Tor-network based darknet market in operation from in and around September 2016 to around September 2017 that sold illegal narcotics and controlled substances, drug paraphernalia, counterfeit and fraud-related goods and services, and other illegal contraband. FinCEN observed Helix conducting 6,871 bitcoin transactions worth $884,507 directly with the darknet marketplace. At least 34 of these direct transactions were for an amount over $2,000. Mr. Harmon failed to file a SAR on these transactions.

30. "Operator of Silk Road 2.0 Website Charged in Manhattan Federal Court," FBI, November 6, 2014, https://www.fbi.gov/contact-us/field-offices/newyork/news/press-releases/operator-of-silk-road-2.0-website-charged-in-manhattan-federal-court.

44. **Unicc.** Unicc was an illicit market in operation from in and around July 2015 to around January 2018 that sold stolen credit card numbers and other fraud-related goods and services, and other illegal contraband. FinCEN observed Helix conducting 134 bitcoin transactions worth over $31,846 directly with the marketplace. FinCEN traced 0.91898767 bitcoin, worth $2,172.51, directly exchanged with Helix from a Unicc associated wallet on June 15, 2017. Mr. Harmon failed to file a SAR on this transaction.

45. **Valhalla Market (Silkkitie).** Valhalla Market (Silkkitie) was a Tor-network based darknet market in operation from in and around July 2015 to around June 2017 that sold illegal narcotics and controlled substances, drug paraphernalia, counterfeit and fraud-related goods and services, and other illegal contraband. Finnish law enforcement seized the market and arrested the site administrators in 2019.[31] FinCEN observed Helix conducting 1,934 bitcoin transactions worth $388,581 directly with the darknet marketplace. At least 27 of these direct transactions were for an amount over $2,000. Mr. Harmon failed to file a SAR on these transactions.

46. **Wall Street Market.** Wall Street Market was a Tor-network based darknet market in operation from in and around November 2016 until May 2019. Wall Street Market was one of the world's largest dark web marketplaces that allowed vendors to sell a wide variety of contraband, including an array of illegal narcotics, counterfeit goods, and malicious computer hacking software. German and US law enforcement seized the market and arrested three administrators on May 3, 2019.[32] Wall Street Market functioned like a conventional e-commerce website. FinCEN observed Helix conducting 279 bitcoin transactions worth $23,964 directly with the darknet marketplace. Mr. Harmon failed to file a SAR on these transactions.

ii. Convertible Virtual Currency Mixing Services

47. Other providers of anonymizing services were found to frequently interact with Helix. Darknet marketplaces actively promote these additional mixers as the primary method for obfuscating bitcoin transactions. FinCEN observed bitcoin transactions equal to $55,617,653 transferred with other mixing service-associated addresses. Of these, FinCEN observed 2,423 direct bitcoin transactions – not including indirect transactions – equal to $2,118,476.43 between Helix and unregistered bitcoin mixing services. At least 261 of these direct transactions were for an amount over $2,000. Mr. Harmon failed to file a SAR on these transactions.

31. "Double Blow To Dark Web Marketplaces," Europol, May 3, 2019, https://www.europol.europa.eu/newsroom/news/double-blow-to-dark-web-marketplaces.
32. "3 Germans Who Allegedly Operated Dark Web Marketplace with Over 1 Million Users Face U.S. Narcotics and Money Laundering Charges," Department of Justice, May 3, 2019, https://www.justice.gov/usao-cdca/pr/3-germans-who-allegedly-operated-dark-web-marketplace-over-1-million-users-face-us.

48. **CVC Mixer 1.** FinCEN observed Helix conducting 1,126 direct bitcoin transactions worth $1,622,807 with CVC Mixer 1. At least 209 of these direct transactions were for amounts over $2,000. Mr. Harmon failed to file SARs on these transactions.

49. **CVC Mixer 2.** FinCEN observed Helix conducting 92 direct bitcoin transactions worth $287,548 with CVC Mixer 2. At least 27 of these direct transactions were for amounts over $2,000. Mr. Harmon failed to file SARs on these transactions.

50. **CVC Mixer 3.** FinCEN observed Helix conducting 52 direct bitcoin transactions worth $42,219 with CVC Mixer 3. At least seven of these direct transactions were for amounts over $2,000. Mr. Harmon failed to file SARs on these transactions.

51. **CVC Mixer 4.** FinCEN observed Helix conducting 1,149 direct bitcoin transactions worth $164,943 with CVC Mixer 4. At least 17 of these direct transactions were for amounts over $2,000. Mr. Harmon failed to file SARs on these transactions.

iii. Darknet Child Exploitation Site

52. Mr. Harmon failed to file a SAR on transactions of convertible virtual currency to a darknet child exploitation site. Users were allowed to send convertible virtual currency into Helix to obfuscate origins of these illicit purchases.

53. **Welcome to Video.** Welcome to Video was a Tor-network based child pornography website, which began operating in or about June 2015 and was shut down by law enforcement on October 16, 2019.[33] Welcome to Video had over 200,000 unique video files, which totaled approximately eight terabytes of data. FinCEN observed Helix conducting at least 73 bitcoin transactions worth over $2,000 directly with Welcome to Video. Mr. Harmon failed to file a SAR on these transaction.

iv. Additional Illicit Proceeds

54. FinCEN observed Helix accepting and transmitting convertible virtual currency for wallets containing the proceeds of various acts of cybercrime. FinCEN traced convertible virtual currencies passing through Helix from these cybercriminal wallets holding value from large scale hacks, account takeovers, criminal organizations and businesses. Many of these transactions contained values greater than or cumulative to $2,000. Mr. Harmon failed to file a SAR on these transactions.

33. "South Korean National and Hundreds of Others Charged Worldwide in the Takedown of the Largest Darknet Child Pornography Website, Which was Funded by Bitcoin," Department of Justice, Oct. 16, 2019, https://www.justice.gov/opa/pr/south-korean-national-and-hundreds-others-charged-worldwide-takedown-largest-darknet-child.

55. **BTC-e.** BTC-e was an unregistered exchanger of convertible virtual currencies that operated from 2011 to July 27, 2017, before it was shut down by a coordinated U.S. government action for alleged money laundering and operating an as unlicensed money transmitter.[34] Concurrently, FinCEN assessed a $110 million dollar civil money penalty against BTC-e and a $12 million dollar civil money penalty against one of its operators, Alexander Vinnik, for failing to register as a money services business, failing to maintain an AML program, and for facilitating millions of dollars of suspicious transactions without filing a SAR.[35] FinCEN observed Helix conducting 1,723 direct bitcoin transactions worth over $904,637 with BTC-e. At least 107 of these direct transactions were for amounts over $2,000. Mr. Harmon failed to file SARs on these transactions.

34. *United States v. BTC-e a/k/a Canton Business Corporation and Alexander Vinnik*, CR 16-00227 SI (N.D. CA. Jan. 17, 2017).
35. *In the matter of BTC-e a/k/a Canton Business Corporation and Alexander Vinnik*, Assessment of Civil Money Penalty Number 2017-03, Financial Crimes Enforcement Network, July 27, 2017.

Department of Justice

U.S. Attorney's Office

Southern District of New York

FOR IMMEDIATE RELEASE

Thursday, October 1, 2020

Founders And Executives Of Off-Shore Cryptocurrency Derivatives Exchange Charged With Violation Of The Bank Secrecy Act

Arthur Hayes, Benjamin Delo, Samuel Reed, and Gregory Dwyer Flouted U.S. Anti-Money Laundering Rules

Audrey Strauss, the Acting United States Attorney for the Southern District of New York, and William F. Sweeney Jr., Assistant Director-in-Charge of the New York Field Office of the Federal Bureau of Investigation ("FBI"), announced the indictment of Arthur Hayes, Benjamin Delo, Samuel Reed, and Gregory Dwyer, charging the four with violating the Bank Secrecy Act and conspiring to violate the Bank Secrecy Act, by willfully failing to establish, implement, and maintain an adequate anti-money laundering ("AML") program at the Bitcoin Mercantile Exchange or "BitMEX." The case is assigned to United States District Judge John G. Koeltl. REED was arrested in Massachusetts this morning, and will be presented in federal court there. HAYES, DELO, and DWYER remain at large.

Acting Manhattan U.S. Attorney Audrey Strauss said: "With the opportunities and advantages of operating a financial institution in the United States comes the obligation for those businesses to do their part to help in driving out crime and corruption. As alleged, these defendants flouted that obligation and undertook to operate a purportedly 'off-shore' crypto exchange while willfully failing to implement and maintain even basic anti-money laundering policies. In so doing, they allegedly allowed BitMEX to operate as a platform in the shadows of the financial markets. Today's indictment is another push by this Office and our partners at the FBI to bring platforms for money laundering into the light."

FBI Assistant Director William F. Sweeney Jr. said: "As we allege here today, the four defendants, through their company's BitMEX crypto-currency trading platform, willfully violated the Bank Secrecy Act by evading U.S. anti-money laundering requirements. One defendant went as far as to brag the company incorporated in a jurisdiction outside the U.S. because bribing regulators in that jurisdiction cost just 'a coconut.' Thanks to the diligent work of our agents, analysts, and partners with the CFTC, they will soon learn the price of their alleged crimes will not be paid with tropical fruit, but rather could result in fines, restitution, and federal prison time."

According to the allegations in the Indictment[1]:

HAYES, DELO, and REED founded BitMEX in or about 2014, and DWYER became BitMEX's first employee in 2015 and later its head of business development. BitMEX, which has long serviced and solicited business from U.S. traders, was required to register with the Commodity Futures Trading Commission ("CFTC") and to establish and maintain an adequate AML program. AML programs ensure that financial institutions, such as BitMEX, are not used for illicit purposes, including money laundering.

Despite those obligations, HAYES, DELO, REED, and DWYER knew by no later than in or about September 2015 that, because BitMEX served U.S. customers, it was required to implement an AML program that included a "know your customer" or "KYC" component, but chose to flout those requirements. Indeed, each of the defendants knew of customers residing in the United States who continued to access BitMEX's trading platform through at least in or about 2018, and that BitMEX policies nominally in place to prevent such trading were toothless or easily overridden to serve BitMEX's bottom line goal of obtaining revenue through the U.S. market without regard to U.S. regulation. While knowing of BitMEX's obligation to implement AML and KYC programs because BitMEX was serving U.S. customers, HAYES, DELO, REED, and DWYER took affirmative steps purportedly designed to exempt BitMEX from the application of U.S. laws such as AML and KYC requirements. For example, the defendants caused BitMEX and its parent corporations formally to incorporate in the Seychelles, a jurisdiction they believed had less stringent regulation and from which they could still serve U.S. customers without performing AML and KYC. Indeed, in or about July 2019, HAYES bragged that the Seychelles was a more friendly jurisdiction for BitMEX because it cost less to bribe Seychellois authorities – just "a coconut" – than it would cost to bribe regulators in the United States and elsewhere.

* * *

HAYES, 34, of Buffalo, New York and Hong Kong, DELO, 36, of the United Kingdom and Hong Kong, REED, 31, of Massachusetts, and DWYER, 37, of Australia and Bermuda, are each charged with one count of violating the Bank Secrecy Act, and one count of conspiring to violate the Bank Secrecy Act, each of which carries a maximum penalty of five years in prison. The maximum potential sentences in this case are prescribed by Congress and are provided here for informational purposes only, as any sentencing of the defendants will be determined by the judge.

Ms. Strauss praised the outstanding investigative work of the FBI's New York Money Laundering Investigation Squad, and the assistance of the FBI's Boston, Milwaukee, and Minneapolis Field Offices. Ms. Strauss also thanked the attorneys and investigators at the CFTC for offering their expertise in the development of this investigation.

The prosecution is being handled by the Office's Money Laundering and Transnational Criminal Enterprises Unit. Assistant U.S. Attorneys Jessica Greenwood and Samuel Raymond are in charge of the prosecution.

[1] As the introductory phrase signifies, the entirety of the text of the Indictment, and the description of the Indictment set forth herein, constitute only allegations, and every fact described should be treated as an allegation.

Attachment(s):
Download Arthur Hayes et al. indictment.pdf

Topic(s):
Financial Fraud

Component(s):
USAO - New York, Southern

Contact:
James Margolin, Nicholas Biase
(212) 637-2600

Press Release Number:
20-218

Updated October 1, 2020