

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

| | | |
|---------------------------------|---|------------------------------------------------|
| UNITED STATES OF AMERICA | : | CRIMINAL NO. |
| | : | |
| v. | : | MAGISTRATE NO. 22-mj-22 (RMM) |
| | : | |
| ILYA LICHTENSTEIN, and | : | <u>VIOLATIONS:</u> |
| HEATHER RHIANNON MORGAN | : | 18 U.S.C. § 1956(h) |
| | : | (Money Laundering Conspiracy) |
| | : | |
| Defendants. | : | 18 U.S.C. § 371 |
| | : | (Money Laundering Conspiracy) |
| | : | |
| | : | 18 U.S.C. § 371 |
| | : | (Conspiracy To Defraud |
| | : | the United States) |
| | : | |
| | : | <u>Criminal Forfeiture:</u> |
| | : | 18 U.S.C. §§ 981(a)(1)(C), 982(a)(1); |
| | : | 28 U.S.C. § 2461(c); 21 U.S.C. § 853(p) |

INFORMATION

The United States Attorney charges that:

At all times relevant to this Information:

COUNT ONE
(Money Laundering Conspiracy)

1. From at least in or around August 2016 through in or around February 2022, in the District of Columbia and elsewhere, the defendant **ILYA LICHTENSTEIN** (“**LICHTENSTEIN**”), together with co-conspirators known and unknown, including Heather Rhiannon Morgan (“Morgan”), did knowingly conspire, combine, confederate, and agree with each other, to violate:

- a. Title 18, United States Code, Section 1956(a)(1)(B)(i), by conducting and attempting to conduct financial transactions affecting interstate commerce, which involved the proceeds of specified unlawful activity, to wit, Wire Fraud,

in violation of Title 18, United States Code, Section 1343, and Computer Fraud and Abuse, in violation of Title 18, United States Code, Section 1030(a)(2)(C) and (a)(4), knowing that the property involved in these financial transactions represented the proceeds of some form of unlawful activity, and knowing that the transactions were designed in whole and in part to conceal and disguise the nature, the location, the source, the ownership, and the control of the proceeds of specified unlawful activity.

Object of the Conspiracy

2. It was the object of the conspiracy for the defendants, **LICHTENSTEIN** and Morgan, to unlawfully enrich themselves by laundering the proceeds of the 2016 hack and scheme to defraud the victim virtual currency exchange, Bitfinex (the “VICTIM VCE”), and to prevent detection of the laundering activity.

Overt Acts

3. In furtherance of the conspiracy, and to accomplish its objects, **LICHTENSTEIN**, Morgan, and others known and unknown committed and caused to be committed various overt acts, including the following:

- a. Beginning in or around January 2017, **LICHTENSTEIN** began to move a portion of the bitcoin (“BTC”) stolen from VICTIM VCE in a series of small, complex transactions across multiple accounts and platforms. This shuffling, which created a voluminous number of transactions, was designed to conceal the path of the stolen funds.
- b. Between on or about August 22, 2016, and on or about April 20, 2017, **LICHTENSTEIN** established multiple accounts at Virtual Currency Exchange

1 (“VCE 1”) using email addresses from an India-based email provider and in the names of third parties unrelated to **LICHTENSTEIN**.

- c. In or around February and March 2017, **LICHTENSTEIN** declined to respond to inquiries from VCE 1’s employees requesting that the registered accountholders for seven of the accounts provide additional identifying information to verify their account ownership. As a result, VCE 1 froze the accounts.
- d. On or about February 28, 2017, in response to inquiries from employees from Virtual Currency Exchange 7 (“VCE 7”) as part of VCE 7’s anti-money laundering and know-your-customer (“AML/KYC”) policies, **LICHTENSTEIN** falsely and fraudulently represented that he would be using his VCE 7 account to trade only his own virtual currency that he had acquired as a result of his early investment in BTC.
- e. In or about February 2018, **LICHTENSTEIN** and Morgan established an account at U.S. Financial Institution 5 (“USFI 5”) for their company, Endpass, and in doing so, represented to USFI 5 that the primary payments into the account would be from software-as-a-service customer payments. In actuality, **LICHTENSTEIN** and Morgan used the account to launder proceeds of the hack of VICTIM VCE.
- f. On or about January 8, 2019, in response to a KYC verification email from employees of Virtual Currency Exchange 10 (“VCE 10”), **LICHTENSTEIN** wrote to representatives from VCE 10, falsely and fraudulently stating that he has “been investing in and mining [BTC] since 2013, so the source of funds

would be those early crypto assets.”

- g. On or about June 27, 2019, in response to an inquiry from a representative from VCE 7 about how her business (SalesFolk) interacted with virtual currency and how her new institutional account would be used, Morgan falsely and fraudulently responded: “SalesFolk has some B2B customers that pay with cryptocurrency,” when in fact that was not the case. Morgan further responded, “Additionally, I also have some personal cryptocurrency of my own that I would like to sell to finance the development of some new software that we are beginning to build. Because the company is an LLC taxed as an S corp it has pass-through taxation and I am the sole owner. I was going to use some of my personal crypto to fund out new software projects.”
- h. On or about July 2, 2019, Morgan further represented to VCE 7 about the source of her cryptocurrency deposits: “My boyfriend (now husband) gifted me cryptocurrency over several years (2014, 2015,), [*sic*] which have appreciated. I have been keeping them in cold storage.” Those funds were in fact the proceeds of the hack of VICTIM VCE.

**(Money Laundering Conspiracy, in violation of
Title 18, United States Code, Section 1956(h))**

COUNT TWO
(Money Laundering Conspiracy)

4. From at least in or around August 2016 through in or around February 2022, in the District of Columbia and elsewhere, the defendant **HEATHER RHIANNON MORGAN** (“**MORGAN**”), together with co-conspirators known and unknown, including Ilya Lichtenstein

(“Lichtenstein”), did knowingly conspire, combine, confederate, and agree with each other, to violate:

- a. Title 18, United States Code, Section 1956(a)(1)(B)(i), by conducting and attempting to conduct financial transactions affecting interstate commerce, which involved the proceeds of specified unlawful activity, to wit, Wire Fraud, in violation of Title 18, United States Code, Section 1343, and Computer Fraud and Abuse, in violation of Title 18, United States Code, Section 1030(a)(2)(C) and (a)(4), knowing that the property involved in these financial transactions represented the proceeds of some form of unlawful activity, and knowing that the transactions were designed in whole and in part to conceal and disguise the nature, the location, the source, the ownership, and the control of the proceeds of specified unlawful activity.

Object of the Conspiracy

5. It was the object of the conspiracy for the defendants, **MORGAN** and Lichtenstein, to unlawfully enrich themselves by laundering the proceeds of the hack and scheme to defraud the victim virtual currency exchange, Bitfinex (the “VICTIM VCE”), and to prevent detection of the laundering activity.

Overt Acts

6. In furtherance of the conspiracy, and to accomplish its objects, the defendants **MORGAN** and Lichtenstein, and others known and unknown to the grand jury, committed and caused to be committed various overt acts, including the overt acts described in Paragraph 3(a)-(h), which are re-alleged and incorporated herein.

**(Conspiracy To Commit Money Laundering,
in violation of Title 18, United States Code, Section 371)**

COUNT THREE
(Conspiracy To Defraud the United States)

7. From at least in or around August 2016, through in or around February 2022, in the District of Columbia and elsewhere, the defendant **HEATHER RHIANNON MORGAN** (“**MORGAN**”), together with co-conspirators known and unknown, including Ilya Lichtenstein (“Lichtenstein”), knowingly and willfully conspired and agreed together and with each other, to defraud the United States and any agency thereof, to wit, the Financial Crimes Enforcement Network (“FinCEN”) of the United States Department of the Treasury in the District of Columbia.

Object of the Conspiracy

8. It was the object of the conspiracy for the defendants, **MORGAN** and Lichtenstein, to unlawfully enrich themselves and facilitate their laundering of fraudulently-obtained proceeds by providing false information to and deceiving virtual currency exchanges and other financial institutions regarding the source of their funds and the nature of their transactions, and thereby to frustrate the AML, KYC, and due diligence efforts by the above-referenced VCEs and other financial institutions, and thereby to prevent the transmission of Suspicious Activity Reports (“SARs”) mandated under the Bank Secrecy Act to FinCEN and the U.S. Department of the Treasury in the District of Columbia.

Overt Acts

9. In furtherance of the conspiracy, and to accomplish its objects, the defendants **MORGAN** and Lichtenstein, and others known and unknown to the grand jury, committed and caused to be committed various overt acts, including the overt acts described in Paragraph 3(a)-(h), which are re-alleged and incorporated herein.

**(Conspiracy To Defraud the United States,
in violation of Title 18, United States Code, Section 371)**

FORFEITURE ALLEGATION

10. Upon conviction of the offense alleged in Count One, the defendant **LICHTENSTEIN** shall forfeit to the United States any property, real or personal, involved in the offense alleged in Count One, and any property traceable thereto, pursuant to Title 18, United States Code, Section 982(a)(1). The United States will also seek a forfeiture money judgment for a sum of money equal to the value of any property, real or personal, involved in Count One, and any property traceable thereto.

11. Upon conviction of the offense alleged in Count Two, the defendant **MORGAN** shall forfeit to the United States any property, real or personal, which constitutes or is derived from proceeds traceable to a violation of the offense alleged in Count Two, pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c). The United States will also seek a forfeiture money judgment for a sum of money equal to the value of any property, real or personal, which constitutes or is derived from proceeds traceable to a violation of the offense alleged in Count Two.

12. The United States will also seek forfeiture of the following specific property upon conviction of the offenses alleged in Count One and Count Two:

- a. Approximately 94,643.29837084 in BTC (after required fees) seized from wallets recovered from defendants’ online storage account and contained in the recipient virtual currency addresses of the following transactions:

| |
|-------------------------------------------------------------------|
| 6e0d701ac2ea3ad87fc8bcaa786b994aa943f5eb9a67a1e345769bb090bf5b9e |
| afdfeeadb9f0a4691cbb8ace33a7c24c052b3608c4c8cc2e25afe053926b6389 |
| 77ad70fadfbbad5191c47c951469095ca845006f25fe9814f30f2853af367459 |
| c49ff6bd054fb386cd02fc94ca34b8773229ed8a5538e023ef7bea772d70c17a |
| 9d06994238d0de958033f42db39a6d2cc0de35e84be0ed080e41f017f02dfffb3 |
| ed1812e8310bb25fbd138aae17be738ad3fa20e0783a8598c8dea56d3be5dad7 |
| ee56a9957f1f6166440bea01d0c0c29e4cec6230bb8231eced6ba844bb095d2a |
| c250725cfc9671d3849a3e85343ec5f3d045f805d002e56725c8ea2aebb9131a |
| b0aa2d76fd9463da6a7aff59e37d7ebf7b6aa1b660de2b2e9ab7755cf6f60ac3 |

| |
|------------------------------------------------------------------|
| b18e40d96906b7b17f337ad6250f0c5aa9db93498832125374102dd2f5e0ed47 |
| 8e5102edd876f71e3482b7602dd9141fbce3ac869fba55a757b4354c70536f34 |
| 11bae40ae4315a1e8f7d9a8df676db6bdb497b153711d1bf7952c540ed1a5966 |
| e6088723889de70fa985e7b8c012c77ea693a6ef9379fb26a951a2bb5c722525 |
| 3fe798be890c7db8beaca9d005cd650e787b1b16bc5e47eef26bfa87124b6a95 |
| d006075f40136ea7733aec2d6f32c31abc09f779de01a33e7e07804907d339c7 |
| 8e53ca8952fbf2d1a272ab376555a1ccee1ff0bcab0747a8c91b0ccfc77cc3fb |
| 97e4eb7ca5d0b2b6d501a53478486d5ed75ce58d1204c6036f25b33439d48627 |
| 658a550600e814f7b7d032b7984912857f37c96a68e4dd3eb1dce4fc774e26f |
| 98281f388a4441d7bb00537e65b1a4581dcaddd3606fc09f6cf19598343be34d |
| d1dbc472abe47902aa71e639ba2feb2098b474ab20b853168ecdb0d87ce02955 |
| 61594a56cd2ef501cdb55b9037cd5785d1ad2eedfb1a4fab7ded50b1052a0650 |
| b7bf853fd6eb27f66963d219d29b85e13796e315473b7c08484335a0b0da7669 |
| 9af41957244e97e70378a7afd2d41b73d0a64d94c9b2df9049c29dd1919741cb |

- b. Approximately 117,376.52651940 in Bitcoin Cash (BCH) (after required fees) seized from wallets recovered from defendants’ online storage account and contained in the recipient virtual currency addresses of the following transactions:

| |
|------------------------------------------------------------------|
| c29fb28633a9bee7720f7ec021c2441dc6a2289c92e887ac5214c35d49314379 |
| 0b9013f818de45ddfa9068f54f8513f15ae35bd711054d119b483a791c750684 |
| 0ae0e3c0db61a2542015164bdcead1636c614bdd5bf51b9537c5b8312db2b84a |
| 16e1ba9b30fd5c86c9dd4ef3967105c2fbfe7ed9f510900b8acd7f7a0a9cddb8 |
| 2544551e053688217ecec544bdc065d502db4ff4f227053fa25cc41be907541 |
| 4f24389c09897d50239d0be3ec39044160f65985cfb3fdf11d117a8fa39aaa24 |
| 6ad1a5ef2ed573b010e7ab32b395bed32142c07bf8bb67534880bbb03591215d |
| 7278e247fc3c7bfa81732ba63c628fe30cb160ec9b7fa357a5dcff8a2f6738e3 |
| 739b58b49039856f8db1da64c713372e04c4e09f9ca32437b639b4d37aad920b |
| 7570b746ecd24f66eb754e100f79c5259e9eecb0c7a0188e6cf5ee84f76d9b21 |
| 7cbd6e7161bbcb80865ef855128bbe1cdeb1e6b87788a99c2559046294bc898f |
| e308fc1199a044f613578e365313008762b8b779b3d92191e6e6ba9a6f5e2182 |
| f8efc360fcd7d6f27b9f7e51911f361b94cb1ff2734be5e301b3cacedda9481e |

- c. Approximately 117,376.58178024 in Bitcoin Satoshi Version (BSV) (after required fees) seized from wallets recovered from defendants’ online storage account and contained in the recipient virtual currency addresses of the following transactions:

| |
|------------------------------------------------------------------|
| 2cf808c73bda45a6ee1c266c60da50f01250d9452f7b51e1caaf3ecec605b416 |
| a0ede2c37597976de79a67db2096b3d8f7a4f60f357c09953a7342ad1948b4b5 |
| 6b46c0067f786acf4f5a1925f12b9860ad61817829f30fef898ad0c3bbaeaf0 |

- d. Approximately 118,102.03258447 in Bitcoin Gold (BTG) (after required fees) seized from wallets recovered from defendants' online storage account and contained in the recipient virtual currency addresses of the following transactions:

| |
|------------------------------------------------------------------|
| a4ba827e99c6cef43ff590457671b63c0d52b2c215797e67c81fc168f499932c |
| 97263227ea621461f3d22132c3e7562b0e401853fd4aced1db1b34aba1a65ab4 |
| 41ad49ad96dfd64eb0293484d4953ccbff7d70839e4c7b75db472c5553db1532 |
| d6e8f7d9aac687cac9af801b4b38cbc8e71db2f21d41f0a6e0d8052d8087456b |
| c2d69e0a0090f201a29d6afb3655b7118b2282146abf64b044481ed99eb2fa27 |
| ec3e2b93e7f7be50bb827ebfd366e2e1f4627dd8ed4550427ec793a3ea20187c |
| 2aa7dbb29d707fb1150c13d1ee6a0a17eeef7326116251cb5d13081fcd297ad8 |
| 70ed72a2c1e2d828f314f5bb327b0e03421bf854c4aba3ea9393258af6fba044 |
| c656cd61fce6c3aebef0f20818d5d092c04c379d3fc72e3ec7e4f019f71a40ec |
| 2238af7a93f797a32ea20492fffa5e27b4d425c46ee7cb0e4fa262e2cddf3142 |
| ec2f4d2e7c13f19657ad4559a9bfd254437989f0f45e8993a17d84c374ecb02f |
| 5e26b7706b1c53b49d99ac1f501971b3d62c6d7e0ba6a01c9791e0d675cfb6e7 |

- e. Approximately 29,016.98 in Monero (XMR) contained within wallets accessible via private keys contained within the defendants' online storage account;
- f. Stolen virtual currency contained within the following wallets:
 0x8CE693CB0626924583931F25f50AF8fC1C6517F0, which holds approximately 8.56 Ether (ETH) and approximately 4,507.99 USD Coin (USDC), as well as various other ERC-20 tokens;
 0x331865e142ACA526B9f75464A2B597ECdaCAF557, which holds approximately 13.88 ETH, approximately 6,656,048 Aave USDC (aUSDC), and approximately 120 Wrapped Ether (WETH), as well as various other tokens; and
 0x3b2Cd27cE5a8633160bC7875B35009f010a51B21, which holds approximately 80 WETH, and approximately .39 ETH.
- g. Approximately .879544 Curve DAO tokens contained within the following address:
 0x612e5774af05cef0626f429d876a315bbdb794fac8fe361ba1d4a01cb3db86a4;
- h. Approximately 1,999,723.976 in Tether (USDT) contained within Yearn Finance Liquidity Pool address 0xaC848276B10B2364fA06C206EE1D059acCD17412, approximately 3,689,545.195 USDT contained within Yearn Finance Liquidity Pool address 0xE2F699AB099e97Db1CF0b13993c31C7ee42FB2ac, and approximately 1,700,000 USDT contained within Yearn Finance Liquidity Pool address 0x6811c26b566e9582B68255B2225917AF96dd8Ec2;
- i. Assorted U.S. and Canadian gold coins excavated and recovered by law enforcement from LOCATION 1, a premises in California known to the defendants and the Government;

- j. Approximately 2,818.199 BTC (after required fees) seized from wallets recovered from Defendants' online storage account;
- k. Approximately 12,267.025 BTC (after required fees) seized from wallets recovered from an external hard drive recovered from the Defendants' residence at 75 Wall Street, Apartment 33M, New York, NY 10005;
- l. Approximately 1,155.901 BTC (after required fees) seized from wallets recovered from Defendants' online storage account and an external hard drive recovered from the Defendants' residence at 75 Wall Street, Apartment 33M, New York, NY 10005;
- m. Approximately 901,014 in USDC (after required fees) seized from wallets recovered from Defendants' online storage account and an external hard drive recovered from the Defendants' residence at 75 Wall Street, Apartment 33M, New York, NY 10005;
- n. Approximately 290,729 USDT (after required fees) seized from wallets recovered from Defendants' online storage account and an external hard drive recovered from the Defendants' residence at 75 Wall Street, Apartment 33M, New York, NY 10005;
- o. Approximately 5,990 USDT (after required fees) seized from wallets recovered from an external hard drive recovered from the Defendants' residence at 75 Wall Street, Apartment 33M, New York, NY 10005;
- p. Approximately 1000.06 in Ether (ETH) (after required fees) seized from wallets recovered from Defendants' online storage account;
- q. Approximately 1,030,436.50 in aUSDT cryptocurrency (after required fees) seized from wallets recovered from Defendants' online storage account and an external hard drive recovered from the Defendants' residence at 75 Wall Street, Apartment 33M, New York, NY 10005;
- r. Approximately 17,572,068.53 in aUSDC cryptocurrency (after required fees) seized from wallets recovered from Defendants' online storage account and an external hard drive recovered from the Defendants' residence at 75 Wall Street, Apartment 33M, New York, NY 10005;
- s. Approximately 3,542,129.56 in Yearn Vault USDT (yvUSDT) cryptocurrency (after required fees) seized from wallets recovered from Defendants' online storage account and an external hard drive recovered from the Defendants' residence at 75 Wall Street, Apartment 33M, New York, NY 10005;
- t. Approximately \$228,266.02 seized from JPMorgan Chase bank account number 877916952;
- u. Approximately 7.998 BTC (after required fees) seized from wallets recovered

from an external hard drive recovered from the Defendants' residence at 75 Wall Street, Apartment 33M, New York, NY 10005;

- v. Approximately 1,770.049 ETH (after required fees) seized from wallets recovered from an external hard drive recovered from the Defendants' residence at 75 Wall Street, Apartment 33M, New York, NY 10005;
- w. Approximately 264.863 BTC (after required fees) seized from wallets recovered from an external hard drive recovered from the Defendants' residence at 75 Wall Street, Apartment 33M, New York, NY 10005;
- x. Approximately \$352,381.55 seized from Wells Fargo bank account number 5361262370;
- y. Approximately 0.196 BTC (after required fees) seized from wallets recovered from an external hard drive recovered from the Defendants' residence at 75 Wall Street, Apartment 33M, New York, NY 10005;
- z. Approximately 1,401.567 ETH (after required fees) seized from wallets recovered from Defendants' online storage account;
- aa. Approximately 1,866.624 ETH (after required fees) seized from wallets recovered from an external hard drive recovered from the Defendants' residence at 75 Wall Street, Apartment 33M, New York, NY 10005;
- bb. Approximately \$2,460,375 seized from the Flagstar bank account corresponding to Signature Bank account number 1503814168; and
- cc. Approximately 1,066 in WETH (after required fees) seized from wallets recovered from defendants' online storage account and an external hard drive recovered from the defendants' residence at 75 Wall Street, Apartment 33M, New York, NY 10005.

13. If any of the property described above as being subject to forfeiture, as a result of any act or omission of the defendants:

- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third party;
- c. has been placed beyond the jurisdiction of the Court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property that cannot be divided without difficulty;

the defendants shall forfeit to the United States any other property of the defendants, up to the value of the property described above, pursuant to Title 21, United States Code, Section 853(p).

(Criminal Forfeiture, pursuant to Title 18, United States Code, Sections 981(a)(1)(C), 982(a)(1); Title 28, United States Code, Section 2461(c); and Title 21, United States Code, Section 853(p))

MATTHEW M. GRAVES
UNITED STATES ATTORNEY
D.C. Bar No. 481052

BY: /s/ Christopher B. Brown
Christopher B. Brown, D.C. Bar No. 1008763
Assistant United States Attorney
U.S. Attorney's Office for the District of Columbia
601 D Street, N.W.
Washington, D.C. 20530
(202) 252-7153
Christopher.Brown6@usdoj.gov

/s/ C. Alden Pelker
Jessica Peck, N.Y. Bar Number 5188248
C. Alden Pelker, Maryland Bar
Trial Attorneys, U.S. Department of Justice
Computer Crime & Intellectual Property Section
1301 New York Ave., N.W., Suite 600
Washington, D.C. 20005
(202) 353-9455 (Peck)
(202) 616-5007 (Pelker)
Jessica.Peck@usdoj.gov
Catherine.Pelker@usdoj.gov