

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA	:	Criminal No. 23-239-1 (CKK)
	:	
v.	:	Case No. 22-mj-22-1 (RMM)
	:	
ILYA LICHTENSTEIN,	:	
	:	
Defendant.	:	

**DEFENDANT ILYA LICHTENSTEIN'S STATEMENT
OF THE OFFENSE AND RELATED CONDUCT**

The defendant ILYA LICHTENSTEIN ("LICHTENSTEIN") admits to the following, which includes information that LICHTENSTEIN has voluntarily disclosed to the government:

1. At all relevant times, the defendant LICHTENSTEIN, also known as "DUTCH" LICHTENSTEIN, was a citizen of Russia and the United States, and a resident of New York and/or California. LICHTENSTEIN was born in Russia, but he moved with his family to the United States when he was a child.

2. At all relevant times, the defendant HEATHER RHIANNON MORGAN ("MORGAN") was a citizen of the United States and a resident of New York and/or California.

3. At all relevant times, LICHTENSTEIN and MORGAN were romantically involved and living together. In or around January 2019, LICHTENSTEIN and MORGAN were married.

4. Bitfinex, also known as the victim virtual currency exchange (the "VICTIM VCE"), was a well-known virtual currency exchange doing business globally.

Background Regarding Virtual Currency

5. Virtual currency is a digital form of value that is circulated over the Internet and is typically not backed by a government. Bitcoin ("BTC") is a decentralized virtual currency. All BTC transactions are posted to a public ledger, the BTC blockchain, accessible via the Internet

and thereby transmitted worldwide, including in the District of Columbia and elsewhere. Although transactions are visible on the public ledger, each transaction is only listed by a series of letters and numbers that does not otherwise identify the individuals involved in the transaction.

6. The storage of virtual currency is typically associated with an individual “wallet,” which is similar to a virtual account. Wallets are used to store and transact in virtual currency. A wallet may include many virtual currency addresses, roughly equivalent to anonymous account numbers.

7. Virtual currency wallets hosted by third parties are referred to as “hosted wallets” because the third party retains a customer’s funds until the customer is ready to transact with those funds. Conversely, wallets that allow users to exercise total, independent control over their funds are called “unhosted” wallets.

The Bank Secrecy Act and FinCEN

8. The Bank Secrecy Act (“BSA”) and its implementing regulations require financial institutions, including U.S.-based banks (“USFIs”) and virtual currency exchanges (“VCEs”) that qualify as “money services businesses” under the BSA (to the extent they operate “wholly or in substantial part within the United States”), to conduct due diligence of their customers and to have anti-money laundering (“AML”) programs in place. *See* 31 C.F.R. § 1010.100(ff).

9. The Financial Crimes Enforcement Network (“FinCEN”), a division of the U.S. Department of Treasury, is responsible for the implementation, administration, and enforcement of the BSA. FinCEN’s website states that its mission is “to safeguard the financial system from illicit use, combat money laundering and its related crimes including terrorism, and promote national security through the strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence.” Financial institutions, as defined by the BSA, are thus

required (1) to collect identifying information about their customers, (2) to verify their clients' identities, and (3) to file reports with FinCEN regarding suspicious activity on their platforms. *See* 31 U.S.C. § 5311 *et seq.*

10. The obligation to report suspicious transactions may be triggered by, among other things, transactions believed to involve funds derived from illegal activity or intended to hide or disguise funds or assets derived from illegal activity; transactions that serve no business or apparent lawful purpose, and for which the financial institution knows of no reasonable explanation after examining the available facts; or transactions that involve the use of the financial institution to facilitate criminal activity. Such reports are commonly known as Suspicious Activity Reports ("SARs").

11. In furtherance of this mission, FinCEN acts as a point of collection for SARs on behalf of the Treasury Department. FinCEN is headquartered in Washington, D.C.

Scheme To Defraud VICTIM VCE

12. Beginning in or around late winter and early spring of 2016, LICHTENSTEIN knowingly and willingly devised a scheme to defraud VICTIM VCE by means of materially false or fraudulent pretenses, representations, or promises. LICHTENSTEIN conducted online research and reconnaissance of the computer infrastructure used by VICTIM VCE. While physically located in the United States, LICHTENSTEIN identified and compromised computer servers belonging to VICTIM VCE outside the United States. LICHTENSTEIN utilized a number of advanced hacking tools and techniques, commonly known as "exploits," to gain unauthorized access to these computer servers. LICHTENSTEIN also used penetration testing software frequently used by cyber criminals, as well as cybersecurity practitioners, because this software

provides data about security vulnerabilities and assists in simulating a cyberattack on a computer system to see how the system would respond.

13. LICHTENSTEIN concealed his activities through a variety of means, including by routing his Internet traffic through the Tor network, through compromised computers that he purchased via a dedicated Remote Desktop Protocol (RDP) marketplace, and through intermediate proxy servers (servers that act as a gateway between users and the Internet), including SOCKS residential proxies rented via online marketplaces. SOCKS or Socket Secure is an Internet protocol that exchanges network packets between a client and server by using a proxy server. LICHTENSTEIN worked late at night to give the appearance that he was operating from another country. Though the servers that LICHTENSTEIN initially compromised did not provide access to virtual currency wallets, LICHTENSTEIN was able to use his access to compromise additional servers and subsequently defeat numerous security measures on VICTIM VCE's network.

14. LICHTENSTEIN ultimately gained access to the keys, or credentials, used to authorize transactions involving virtual currencies held by VICTIM VCE, including funds belonging to customers of VICTIM VCE. In or about August 2016, LICHTENSTEIN used his access to VICTIM VCE's keys to fraudulently authorize more than 2,000 transactions in which approximately 119,754 BTC was transferred from VICTIM VCE's wallets to an outside wallet ("Wallet 1CGA4s") under LICHTENSTEIN's custody and control. At the time of the hack, the stolen virtual currency was valued at approximately \$71 million.

15. Following the hack, LICHTENSTEIN took steps to conceal his activity, including by returning to VICTIM VCE's computer systems and deleting access credentials and certain log files that might lead investigators to determine that someone had gained unauthorized access. In the course of the hack, LICHTENSTEIN, while located in the United States, transmitted and

caused to be transmitted writings, signs, and signals by means of wire communication in interstate and foreign commerce over the Internet to VICTIM VCE's computer servers located outside the United States.

16. During the course of the reconnaissance phase of the hack of VICTIM VCE, LICHTENSTEIN gained unauthorized access to VICTIM VCE's customer login credentials. LICHTENSTEIN used these customer credentials to engage in credential spraying—that is, using the customer credentials stolen from VICTIM VCE to attempt to log into other accounts—targeting user accounts at other virtual currency exchanges. As a result of these efforts, LICHTENSTEIN fraudulently obtained access to customer accounts at a second virtual currency exchange, VCE A, and stole an estimated several hundred thousand dollars' worth of funds from VCE A customer accounts. LICHTENSTEIN commingled these funds with the funds stolen from VICTIM VCE.

17. Prior to the hack of VICTIM VCE, LICHTENSTEIN engaged in earlier, less significant hacking and financial fraud activity, including as a juvenile. LICHTENSTEIN developed an interest in virtual currency and darknet markets, including through various illicit transactions on darknet markets. Prior to 2016, and separate from his theft from VICTIM VCE, LICHTENSTEIN located credentials to VCE A's application programming interface (API) that allowed him to withdraw funds through the exchange's API. LICHTENSTEIN used this access to steal approximately \$200,000 from VCE A. In addition, in or around 2015, LICHTENSTEIN illicitly obtained and transferred a small amount of PayCoin, an alternative form of virtual currency.

The Money Laundering Conspiracy and Conspiracy To Defraud

18. LICHTENSTEIN studied how transactions are traced on the blockchain and formulated a detailed plan that was designed to reduce any perceived illicit taint of the funds over time.

19. First, LICHTENSTEIN left the stolen funds sitting dormant in Wallet 1CGA4s until, beginning in or around January 2017, when LICHTENSTEIN began to move a portion of the stolen BTC out of Wallet 1CGA4s 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 BTC, making it difficult for law enforcement to trace the funds. Next, LICHTENSTEIN moved some of the stolen funds from Wallet 1CGA4s to another large staging wallet; from the staging wallet into other wallets, which were not otherwise linked or associated; through numerous accounts at multiple darknet marketplaces, including AlphaBay and Hydra, using multiple segregated input and withdrawal addresses; and through coinjoins, mixers, and exchanges that did not require know-your-customer (KYC) information about their users.

20. Following the hack, LICHTENSTEIN enlisted MORGAN's help in laundering the stolen funds. MORGAN was initially unaware of the specific origin of LICHTENSTEIN's proceeds, although she participated with LICHTENSTEIN in efforts to conceal and obscure the source of the funds while knowing and understanding that the funds were the result of some unspecified unlawful and fraudulent activity. Sometime after the hack, but by no later than in or around early 2020, LICHTENSTEIN explicitly told MORGAN that LICHTENSTEIN was responsible for the 2016 hack of VICTIM VCE.

21. The following steps were taken in furtherance of the money laundering scheme:

- a. Setting up numerous accounts at USFIs and VCEs to stay below transaction thresholds that would require enhanced customer due diligence by financial institutions;
- b. Converting stolen funds into fiat currency through Russian and Ukrainian bank accounts and then withdrawing the laundered funds at U.S.-based ATMs;
- c. Converting stolen BTC into a virtual currency named Monero (XMR), which is an anonymity-enhancing virtual currency with a nontransparent blockchain, via exchanges that did not require KYC;
- d. Using intermediate, unhosted wallets to avoid exchange-to-exchange transactions that would undermine the anonymity benefits of using XMR, darknet markets, and coinjoins/mixers, such as Bitcoin Fog, Helix, and ChipMixer;
- e. Converting a portion of the stolen funds to Tether (USDT) and USD Coin (USDC), which are both stablecoins pegged to the U.S. dollar, as a means of avoiding the price volatility associated with holding other virtual currencies, such as BTC, the price of which fluctuates daily;
- f. Using exchanges with high sale limits and setting up multiple accounts at numerous exchanges in order to launder large amounts stolen of funds;
- g. Using pre-existing, KYC-verified accounts purchased from illicit vendors offering profiles designed to defeat exchange AML controls; and
- h. Using accounts at USFIs and VCEs opened under LICHTENSTEIN's and MORGAN's true names and/or the names of their businesses, including

accounts at “VCE 5,” “VCE 6,” “VCE 7,” “VCE 8,” “VCE 9,” and “VCE 10”;
and

- i. Converting a portion of the stolen funds into gold coins, which were further concealed by MORGAN when she buried them at a location that has since been disclosed to law enforcement, which has recovered the gold coins in full.

22. In engaging in the above-referenced conduct, LICHTENSTEIN, at times with MORGAN’s assistance, employed numerous money laundering techniques, including, but not limited to: (1) using accounts set up with fictitious identities; (2) moving the stolen funds in a series of small amounts, totaling thousands of transactions, as opposed to moving the funds all at once or in larger amounts; (3) utilizing computer programs to automate transactions, a laundering technique that allows for many transactions to take place in a short period of time; (4) layering the stolen funds by depositing them into accounts at a variety of VCEs and darknet markets and then withdrawing the funds, which obfuscates the trail of the transaction history by breaking up the fund flow; (5) converting the BTC to other forms of virtual currency, including anonymity-enhanced virtual currency, in a practice known as “chain hopping”; and (6) using U.S.-based business accounts to legitimize activity. MORGAN further assisted LICHTENSTEIN with setting up accounts with fictitious identities and using U.S.-based business accounts to legitimize the laundering transactions.

23. Additionally, over the course of their conspiracy, LICHTENSTEIN, at times with MORGAN’s assistance, converted stolen funds through the use of debit cards linked to foreign bank accounts. The foreign bank accounts were registered to Russian and Ukrainian money mules, who worked for brokers and who typically created the accounts in-person at the foreign banks. The accounts were then offered for sale by brokers on darknet markets and cybercriminal forums.

LICHTENSTEIN acquired numerous accounts through such platforms. The purchased account packages included a debit card, as well as identity document scans and the SIM cards associated with the phone used to establish the account. LICHTENSTEIN had the packages delivered to him during trips with MORGAN to Kazakhstan and Ukraine. The packages were typically shipped via a shipping service or handed off by a courier in a prearranged public meeting place, such as a train station. LICHTENSTEIN then sent BTC to Russian- and Eastern-European-based instant exchange platforms, which converted the BTC to fiat currency and deposited the corresponding fiat funds into the Russian and Ukrainian bank accounts. LICHTENSTEIN and MORGAN would travel to ATMs in the United States and use the purchased debit cards to withdraw funds. LICHTENSTEIN and MORGAN would bring multiple cards per trip, and used only one card per ATM to avoid suspicion.

24. In or around November 2021, LICHTENSTEIN and MORGAN learned that records related to an account held by LICHTENSTEIN and used in furtherance of the conspiracy had been disclosed to U.S. law enforcement. The provider controlling the account failed to process a valid and timely extension of a non-disclosure order issued by the U.S. District Court for the District of Columbia and notified LICHTENSTEIN in violation of the court order. Upon receipt of the notice, LICHTENSTEIN and MORGAN took steps to further conceal their activity. For example, LICHTENSTEIN deleted data from devices in the United States and abroad, and LICHTENSTEIN and MORGAN threw a computing device down a garbage chute, when said computing device contained relevant, inculpatory evidence related to this criminal scheme.

**False Statements and Deceptions Targeting Virtual Currency Exchanges
and Other U.S. Financial Institutions**

25. During the period from in or around August 2016 through in or around February 2022, LICHTENSTEIN and MORGAN used false and fictitious identifying information to

establish accounts, made false and fraudulent representations, and lied to and deceived VCEs and other U.S. financial institutions that they used to launder the illegal proceeds of the 2016 hack of VICTIM VCE, including the following:

- a. Between on or about August 22, 2016, and on or about April 20, 2017, LICHTENSTEIN established multiple accounts at VCE 1 using email addresses from the same India-based email provider and in the names of third parties unrelated to LICHTENSTEIN.
- b. 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.
- c. On or about February 28, 2017, in response to inquiries from employees from VCE 7 as part of VCE 7's 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.
- d. In or about February 2018, LICHTENSTEIN established an account at USFI 5 for LICHTENSTEIN and MORGAN's 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 the proceeds of the hack of VICTIM VCE.

- e. On or about January 8, 2019, in response to a KYC verification email from 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.”
- f. 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.”
- g. 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 proceeds of the hack of VICTIM VCE.

26. At all times relevant to this indictment, VCE 1, VCE 7, VCE 10, and USFI 5 were financial institutions doing business in the United States, were subject to the Bank Secrecy Act, and were registered with FinCEN.

27. Each of the accounts referenced above was used by LICHTENSTEIN and MORGAN to launder the illegal proceeds of the 2016 hack of VICTIM VCE, and the government's tracing has shown that the majority of funds deposited into each account was derived directly or indirectly from the same stolen funds. One purpose of LICHTENSTEIN and MORGAN's deceptions was 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 SARs mandated under the Bank Secrecy Act to FinCEN and the U.S. Department of the Treasury in the District of Columbia.

Conclusion

28. LICHTENSTEIN admits that some of the proceeds he personally obtained as a result of the offenses described above have been dissipated by him and cannot be located upon the exercise of due diligence; have been transferred or sold to, or deposited with, a third party; and/or have been placed beyond the jurisdiction of the Court.

29. LICHTENSTEIN acknowledges that the specific properties listed in the Consent Order of Forfeiture are proceeds of and/or property involved in this money laundering conspiracy.

30. LICHTENSTEIN waives any challenge to venue in the District of Columbia.

31. The facts contained herein are not complete in all details. Instead, they are provided in order to demonstrate that the elements of the charged offenses have been met for purposes of a plea in this case. These are not all of the facts known to the defendants and to the government.

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

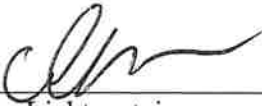
BY: /s/ Christopher B. Brown
Christopher B. Brown, D.C. Bar No. 1008763
Assistant United States Attorney
U.S. Attorney's Office for the District of Columbia
601 D Street, N.W.
Washington, D.C. 20530
(202) 252-7153
Christopher.Brown6@usdoj.gov

/s/ Jessica C. Peck
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

Defendant's Acceptance

I have read this Statement of the Offense and carefully reviewed every part of it with my attorneys. I am fully satisfied with the legal services provided by my attorney in connection with this Statement of the Offense and all matters relating to it. I fully understand this Statement of the Offense and voluntarily agree to it. No threats have been made to me, nor am I under the influence of anything that could impede my ability to understand this Statement of the Offense fully. No agreements, promises, understandings, or representations have been made with, to, or for me other than those set forth above.

Date: 8/2/23

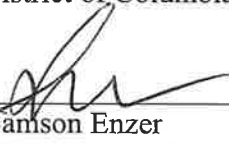


Ilya Lichtenstein
Defendant

Defense Counsel's Acknowledgment

I have reviewed every part of this Statement of the Offense with my client. It accurately and completely sets forth the Statement of the Offense agreed to by the defendant and the Office of the United States Attorney for the District of Columbia.

Date: 8/2/23



Samson Enzer
Anirudh Bansal
Connor O'Shea
Angela F. Collins
Attorneys for Defendant