

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

UNITED STATES OF AMERICA	:	
	:	
v.	:	Criminal No. 19-cr-395 (BAH)
	:	
LARRY DEAN HARMON,	:	
	:	
Defendant.	:	

STATEMENT OF THE OFFENSE AND RELATED CONDUCT

I. THE ELEMENTS OF THE OFFENSES

Conspiracy To Launder Monetary Instruments: The essential elements of the offense of Conspiracy To Launder Monetary Instruments, in violation of Title 18, United States Code, Section 1956(h), each of which the government must prove beyond a reasonable doubt to sustain a conviction, are:

- (1) that an agreement existed between two or more people to commit an act in violation of (a) Title 18, United States Code, Section 1956(a)(1)(A)(i), or (b) Title 18, United States Code, Section 1956(a)(1)(B)(i); and
- (2) that the defendant intentionally joined in that agreement.

The essential elements of promotional money laundering, in violation of Title 18, United States Code, Section 1956(a)(1)(A)(i), are:

- (1) that the defendant knowingly conducted or tried to conduct a financial transaction;
- (2) that the defendant knew that the money or property involved in the transaction was the proceeds of some kind of unlawful activity;
- (3) that the money or property did come from an unlawful activity, specifically the felonious manufacture, importation, receiving, concealment, buying, selling, or otherwise dealing in

a controlled substance or listed chemical, in violation of Title 21, United States Code, Sections 841(a)(1) and 846; and

- (4) that the defendant the defendant acted with intent to promote the carrying on of specified unlawful activity, specifically the felonious manufacture, importation, receiving, concealment, buying, selling, or otherwise dealing in a controlled substance or listed chemical, in violation of Title 21, United States Code, Sections 841(a)(1) and 846.

The essential elements of concealment money laundering, in violation of Title 18, United States Code, Section 1956(a)(1)(B)(i), are:

- (1) that the defendant knowingly conducted or tried to conduct a financial transaction;
- (2) that the defendant knew that the money or property involved in the transaction was the proceeds of some kind of unlawful activity;
- (3) that the money or property did come from an unlawful activity, specifically the felonious manufacture, importation, receiving, concealment, buying, selling, or otherwise dealing in a controlled substance or listed chemical, in violation of Title 21, United States Code, Sections 841(a)(1) and 846; and
- (4) that the defendant knew that the transaction was designed, in whole or in part, to conceal or disguise the nature, location, source, ownership, or the control of the proceeds.

II. FACTUAL BASIS

Had this case proceeded to trial, the government would have proven the following facts beyond a reasonable doubt:

1. At all relevant times, the defendant LARRY DEAN HARMON (“HARMON”) was a resident of Ohio and maintained a residence in Belize.

2. Starting in or about April 2014, HARMON owned and operated a Darknet search engine called Grams. The Darknet refers to a collection of hidden websites whose locations are anonymized by the use of the Tor network, a network of globally distributed relay computers that anonymizes users' Internet traffic. The Darknet includes a number of criminal platforms that sell illegal goods, like guns and drugs, and criminal services, like hacking and money laundering. In or about July 2014, HARMON posted online that he believed the Darknet primarily sold drugs and illegal items.

3. Starting in or about July 2014, HARMON owned and operated a money transmitting business and money laundering service called Helix. Helix was a service linked to and affiliated with Grams, HARMON's Darknet search engine. HARMON offered two versions of Helix, namely, Helix, which required a customer to have a Grams account, and Helix Lite, which did not require a Grams account. Helix offered an Internet-based service that was accessible in the District of Columbia and other States.

4. Both versions of Helix enabled customers, for a fee, to send bitcoins to designated recipients in a manner which was designed to conceal and obfuscate the source or owner of the bitcoins. This type of service is commonly referred to as a bitcoin "mixer" or "tumbler." A Helix customer was required to send their bitcoins to a bitcoin wallet controlled by Helix. In turn, Helix would transmit bitcoins located in other bitcoin wallets controlled by Helix, which Helix advertised were not linked to Darknet activity, to a receiving address designated by the customer. In practice, this allowed customers to transmit bitcoins to other persons and to other bitcoin addresses without leaving a direct trail of transactions on the public blockchain.

5. Helix was advertised to customers on the Darknet as a way to conceal transactions from law enforcement. In or about June 2014, shortly before launching Helix, HARMON posted

online that Helix was designed to be a “bitcoin tumbler” that “cleans” bitcoins by providing customers with new bitcoins “which have never been to the darknet before.” In or about August 2014, HARMON posted online that “Helix uses new addresses for each transaction so there is no way LE would be able [*sic*] to tell which addresses are helix addresses,” referring to law enforcement by the acronym LE. In or about March 2015, HARMON posted online: “No one has ever been arrested just through bitcoin taint, but it is possible and do you want to be the first? . . . Most markets use ‘Hot Wallets’, they put all their fees in these wallets. LE just needs to check the taints on these wallets to find all the addresses a market uses.”

6. HARMON conspired with Darknet vendors and marketplace administrative teams to launder bitcoins generated through illegal drug trafficking offenses through Helix, for the purpose of concealing the location, source and ownership or control of such “dirty” bitcoins, and thereby to promote the continued prosperity of illegal Darknet markets and vendors engaged in such offenses.

7. In furtherance of the conspiracy, Helix partnered with several Darknet markets, including AlphaBay, to provide bitcoin money laundering services for market customers. AlphaBay was a Darknet market in operation from in or about December 2014 through in or about July 2017, when the site was seized by law enforcement. 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 Grams-Helix. Similarly, HARMON modified a feature of Helix to ensure compatibility with transactions executed on the Darknet market Evolution, another criminal platform offering illegal

drugs, as well as other illegal goods including counterfeit and fraud-related goods and services. HARMON communicated about the Helix feature with Evolution’s administrators, who, in turn, agreed to promote Helix as a “great method” to conduct transactions on their website. HARMON developed an Application Program Interface (API) to allow Darknet markets to integrate Helix directly into their bitcoin withdrawal systems, and at least one Darknet market, Cloud 9, successfully integrated Helix using the API.

8. On or about November 8, 2016, a Federal Bureau of Investigation (FBI) employee acting in an undercover capacity from a location in the District of Columbia transferred 0.16 bitcoin from an AlphaBay bitcoin wallet to Helix. Helix then exchanged the bitcoin for an equivalent amount of bitcoin, less a 2.5 percent fee, which was not directly traceable to AlphaBay.

9. In total, Helix exchanged at least approximately 354,468 bitcoins—the equivalent of approximately \$311,145,854 million in U.S. dollars at the time of the transactions—on behalf of its customers, including customers in the District of Columbia. HARMON retained a percentage of these transactions as his commissions and fees for operating Helix. The largest identifiable customers sending bitcoins directly to Helix were Darknet markets selling illegal goods and services, including AlphaBay, Agora Market, Nucleus, and Dream Market, and other Darknet markets.

10. HARMON began to shut down operations for Grams and Helix in or about December 2017.

11. At all relevant times, Helix was not licensed as a money transmitter within the District of Columbia, as required under the District of Columbia Money Transmitters Act, D.C. Code § 26-1023(c), despite engaging in the business of money transmission within the District of Columbia.

12. At all relevant times, Helix was not registered with the Financial Crimes Enforcement Network (“FinCEN”), a division of the U.S. Department of the Treasury, as required under the Bank Secrecy Act, 18 U.S.C. § 5330, and its implementing regulations, despite operating as a money transmitting business within the District of Columbia and elsewhere.

III. CONCLUSION

13. The property involved in the money laundering conspiracy described above totaled at least 354,468 bitcoins (BTC), which was the equivalent of approximately \$311,145,854 in U.S. dollars at the time of the transactions.

14. HARMON waives any challenge to venue in the District of Columbia.

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

CHANNING D. PHILLIPS
ACTING UNITED STATES ATTORNEY
D.C. Bar No. 415793

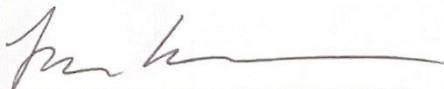
BY: /s/ Christopher B. Brown
Christopher B. Brown, D.C. Bar No. 1008763
Assistant United States Attorney
U.S. Attorney’s Office for the District of Columbia
555 4th Street, N.W.
Washington, D.C. 20530
(202) 252-7153
Christopher.Brown6@usdoj.gov

/s/ C. Alden Pelker
C. Alden Pelker, Maryland Bar
Trial Attorney, U.S. Department of Justice
1301 New York Ave., N.W., Suite 600
Washington, D.C. 20005
(202) 616-5007
Catherine.Pelker@usdoj.gov

Defendant's Acceptance

I have read this Statement of the Offense and carefully reviewed every part of it with my attorney. 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: 8-10-21

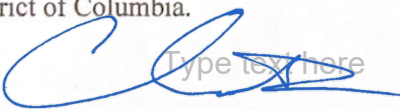


Larry Dean Harmon
Defendant

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: 8/10/21



Charles Flood, Esq.
Attorney for Defendant