SEALED

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

Holding a Criminal Term
Grand Jury Sworn in on May 7, 2019

UNITED STATES OF AMERICA	:	**SEALED INDICTMENT**
	:	
	:	**Criminal No.**
	:	
v.	:	**Count One: 18 U.S.C. § 1956(h)**
	:	**(Conspiracy To Launder**
	:	**Monetary Instruments)**
LARRY DEAN HARMON,	:	
	:	**Count Two: 18 U.S.C. § 1960(a)**
	:	**(Operating an Unlicensed Money**
	:	**Transmitting Business)**
	:	
	:	**Count Three: D.C. Code § 26-1023(c)**
	:	**(Money Transmission Without a**
	:	**License)**
	:	
	:	**Forfeiture: 18 U.S.C. § 982(a)(1);**
	:	**21 U.S.C. § 853(p)**

INDICTMENT

The Grand Jury Charges:

Case No.19-cr-00395
Assigned to: Chief Judge Beryl A. Howell
Assign. Date: 12/3/2019
Description: INDICTMENT (B)

INTRODUCTION

At all times material to this indictment:

1. Defendant LARRY DEAN HARMON ("HARMON") was a resident of Ohio and 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 available through a network of globally distributed relay computers called the Tor network. They are hidden websites because, unlike standard Internet websites, on the Tor network there is no publicly available listing of the Internet Protocol (IP) addresses of servers hosting websites on the Tor network. The Darknet

includes a number of hidden websites that sell illegal goods, like guns and drugs, and 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 and money laundering business called Helix. Helix was a service linked to and affiliated with Grams, HARMON's Darknet search engine, and the two services were sometimes referred to collectively as Grams-Helix. Helix offered an Internet-based service that was accessible in the District of Columbia and other States.

4. 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."

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 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. From at least in or about November 2016, Helix partnered with the Darknet market AlphaBay to provide bitcoin money laundering services for AlphaBay customers. AlphaBay was