

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA,
c/o U.S. Attorney's Office for D.C.
Civil Division
601 D Street, NW
Washington, DC 20530,

Plaintiff,

v.

LARRY DEAN HARMON (d/b/a Helix),
3853 Yellow Creek Rd.
Akron, OH 44333,

Defendant.

Civil Action No. 22-3203

COMPLAINT

1. The United States of America (“United States” or “Government”) brings this action against Larry Dean Harmon (d/b/a Helix) (“Harmon”) to recover a civil money penalty imposed under 31 U.S.C. §§ 5311-5314, 5316-5332 and 12 U.S.C. §§ 1829b, 1951-1959, collectively referred to as the Bank Secrecy Act.

JURISDICTION AND VENUE

2. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. §§ 1331 and 1345.

3. The Court may exercise personal jurisdiction over Harmon because he transacted business in this District.

4. Venue is proper in the District of Columbia under 28 U.S.C. § 1395 because the claim in this matter accrued in this District, and Harmon is found in this District, having transacted business in it.

PARTIES

5. The United States brings this action on behalf of the Department of the Treasury, including its component, the Financial Crimes Enforcement Network (“FinCEN”).

6. At all relevant times to this complaint, Harmon was a resident of Ohio and maintained a residence in Belize. At all times relevant to this complaint, Harmon offered Internet-based money transmission services accessible to and used by individuals in this District.

STATUTORY AND REGULATORY BACKGROUND

7. FinCEN, a bureau within the Department of the Treasury, administers the Bank Secrecy Act pursuant to authority delegated by the Secretary of the Treasury. *See* Treasury Order 180-01 (July 1, 2014).

8. The Bank Secrecy Act requires the filing of reports and the maintenance of records useful in criminal, tax, or regulatory investigations or proceedings, or in the conduct of intelligence or counterintelligence activities to protect against international terrorism.

9. Regulations implementing the Bank Secrecy Act appear at 31 C.F.R. Chapter X. Rules issued under the Bank Secrecy Act require each money services business to: (i) register with FinCEN, (ii) file Suspicious Activity Reports (also called “SARs”); (iii) implement an anti-money laundering program, and (iv) maintain records related to transmittals of funds.

10. FinCEN may impose a civil monetary penalty “at any time before the end of the 6-year period beginning on the date of the transaction with respect to which the penalty was assessed,” and may commence an action to recover the civil money penalty at any time before the end of the 2-year period beginning on the date the penalty was imposed. 31 U.S.C. §§ 5321(b), 5330(e).

11. Money services businesses are “financial institutions” for purposes of the Bank Secrecy Act and its implementing regulations. *See* 31 U.S.C. §§ 5312(a)(2)(J), (K), (R); 31 C.F.R. § 1010.100(t)(3).

12. A “money services business” is defined in regulations implementing the Bank Secrecy Act to include persons who are engaged as a business in providing money transmission services “wholly or in substantial part within the United States.” 31 C.F.R. § 1010.100(ff).

13. 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). *See also* FIN-2013-G001, “Application of FinCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies” (Mar. 18, 2013); FIN-2019-G001, “Application of FinCEN’s Regulations to Certain Business Models Involving Convertible Virtual Currencies” (May 9, 2019).

14. Providers of anonymizing services, commonly referred to as “mixers” or “tumblers,” are either persons that accept convertible virtual currencies or retransmit them in a manner designed to prevent others from tracing the transmission back to its source.

15. Providers of anonymizing services are money transmitters under FinCEN regulations because it accepts and transmits convertible virtual currencies. *See* FIN-2019-G001, “Application of FinCEN’s Regulations to Certain Business Models Involving Convertible Virtual Currencies” (May 9, 2019) at 19-20.

16. FinCEN may impose on any person who owns or controls an unregistered money services business a civil money penalty for each day that the money services business remains unregistered. *See* 31 U.S.C. § 5330(e)(2); 31 C.F.R. § 1022.380(e).

17. As of October 19, 2021, FinCEN could assess a penalty of up to \$7,954 for each money services business registration violation occurring on or before November 2, 2015. *See* 31 C.F.R. § 1010.821 (2021).

18. As of October 19, 2021, FinCEN could assess a penalty of up to \$8,084 for each violation occurring after November 2, 2015. *Id.* Each day a violation continues constitutes a separate violation. 31 C.F.R. § 1022.380(e).

19. FinCEN may impose a civil money penalty on a domestic financial institution that willfully violates the Bank Secrecy Act by failing to establish or maintain an adequate anti-money laundering program and for failing to file Suspicious Activity Reports as appropriate, and on any partner, director, officer, or employee who willfully participates in the violation. *See* 31 U.S.C. § 5321(a)(1); 31 C.F.R. § 1010.820.

20. The term “domestic” refers to “the doing of business within the United States” or the performance of functions within the United States. 31 C.F.R. § 1010.100(o); *see also* 31 U.S.C. § 5312(b)(1).

21. For violations occurring on or before November 2, 2015, FinCEN may impose a penalty of \$25,000 to \$100,000 for willful violations of Bank Secrecy Act program requirements. *See* 31 U.S.C. § 5321(a)(1); 31 C.F.R. § 1010.820(f).

22. As of October 19, 2021, FinCEN could assess a penalty of \$54,789 to \$219,156 for anti-money laundering program violations after November 2, 2015. *See* 31 C.F.R. § 1010.821 (2021). For violations of the requirement to implement an adequate anti-money laundering program, “a separate violation occurs for each day that the violation continues.” 31 U.S.C. § 5321(a)(1); 31 C.F.R. § 1010.821.

FACTUAL ALLEGATIONS

I. BITCOIN AND DIGITAL CURRENCIES

23. Bitcoin is a form of decentralized, convertible digital currency that exists using an online, decentralized ledger system. Bitcoin is just one of many forms of digital currency. There are many others, including litecoin, ether, and dogecoin; however, bitcoin has the largest market capitalization of any present form of decentralized digital currency.

24. While bitcoin is an internet-based form of currency, it is possible to “print out” the necessary bitcoin information and exchange it via physical media. Bitcoin is not issued by any government, bank, or company, but rather is generated and controlled through computer software operating via a decentralized network. To acquire bitcoin, a typical user will purchase it from a bitcoin seller or “exchanger.”

25. Bitcoin exchangers typically accept payments of fiat currency (currency which derives its value from government regulation or law), or other convertible digital currencies. When a user wishes to purchase bitcoin from an exchanger, the user will typically send payment in the form of fiat currency, often via bank wire or automated clearing house (i.e., “ACH”) transfer, for the corresponding quantity of bitcoin, based on a fluctuating exchange rate. The exchanger, often for a commission, will then attempt to broker the purchase with another user of the exchange that is trying to sell bitcoin, or, in some instances, will act as the seller itself.

26. When a user acquires bitcoin, ownership of the bitcoin is transferred to the user’s bitcoin address. The bitcoin address is somewhat analogous to a bank account number and is comprised of a case-sensitive string of letters and numbers amounting to a total of 26 to 35 characters. The user can then conduct transactions with other bitcoin users by transferring bitcoin to their bitcoin addresses via the internet.

27. Little to no personally identifiable information about the payer or payee is transmitted in a bitcoin transaction itself. Bitcoin transactions occur using a public key and a private key. A public key is used to receive bitcoin, and a private key is used to allow withdrawals from a bitcoin address. Only the bitcoin address of the receiving party and the sender's private key are needed to complete the transaction. These two keys by themselves rarely reflect any information identifying the payer or payee.

28. All bitcoin transactions are recorded on what is known as the Blockchain. The Blockchain is a distributed public ledger that maintains all bitcoin transactions, incoming and outgoing. The Blockchain records every bitcoin address that has ever received a bitcoin and maintains records of every transaction for each bitcoin address. In some circumstances, bitcoin payments may be effectively traced by analyzing the Blockchain.

II. HARMON, HELIX, AND COIN NINJA

29. On or about June 2014, Harmon began operating and administering a convertible virtual currency exchanger called Helix. Harmon was the primary administrator and operator of Helix.

30. Harmon, doing business as Helix, accepted bitcoin and transmitted bitcoin to another person or location by a variety of means. 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.

31. Beginning on or about June 6, 2014, through on or about December 16, 2017, 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.

32. Beginning on or about July 13, 2017, Harmon became Chief Executive Officer of Coin Ninja LLC (“Coin Ninja”), a Delaware-incorporated and Ohio-located money transmitter that operates as an exchanger of convertible virtual currencies. Harmon participated in the direction and supervision of Coin Ninja’s operations and finances.

33. On or about July 13, 2017, Harmon, through his legal representative, registered Coin Ninja in Delaware. Harmon later filed a corporate registration in Ohio on November 8, 2017. Harmon was the Chief Executive Officer of Coin Ninja, which operated as a money services business.

34. Harmon willfully participated in the direction and supervision of Coin Ninja’s operations and finances. Coin Ninja stated on the Frequently Asked Questions (or “FAQ”) page of its website that it also provided a “mixing” service.

35. Coin Ninja also offered a service called DropBit, which described itself as “like Venmo for Bitcoin,” allowing customers to accept and transmit bitcoin through text messages or Twitter handles. Harmon advertised Coin Ninja’s DropBit service as a service that helps circumvent know your customer procedures.

III. CRIMINAL CASE

36. On December 3, 2019, Harmon was indicted in the District of Columbia for conspiracy to launder monetary instruments in violation of 18 U.S.C. § 1956, for the operation of an unlicensed money transmitting business in violation of 18 U.S.C. § 1960, and for engaging in money transmission without a license in violation of D.C. Code § 26-1023(c). *United States v. Harmon*, Crim. No. 19-0395 (BAH) (D.D.C. filed Dec. 3, 2019), ECF No. 1 (Indictment).

37. On August 18, 2021, Harmon pled guilty to conspiring to launder monetary instruments in violation of 18 U.S.C. § 1956. *Id.* at ECF Nos. 122, 123 (Statement of Offense and Plea Agreement).

IV. FINCEN'S CIVIL MONEY PENALTY

38. As detailed in the Assessment of Civil Money Penalty issued on October 19, 2020 (attached hereto as Exhibit 1), FinCEN assessed monetary penalties against Harmon for the following conduct.

A. Failure to Register as A Money Services Business

39. A money services business is any person or entity that receives something of value (including currency or value that substitutes for currency) from one person and transmits either the same or a different form of value to another person or location by any means. 31 C.F.R. § 1010.100(ff); 2011 Money Services Business Final Rule, 76 Fed. Reg. 43,585, 43,596 (July 21, 2011).

40. A money services business is required to register with FinCEN within 180 days of beginning operation and to renew such registration every two years. 31 U.S.C. § 5330; 31 C.F.R. § 1022.380(b)(2).

41. Harmon, doing business as Helix, operated as an exchanger of convertible virtual currencies, accepting and transmitting bitcoin to another person or location by a variety of means.

42. Harmon began operating Helix in June 2014 and ceased operations in December 2017.

43. Harmon never registered as a money services business with FinCEN.

44. Before closing Helix, Harmon began operating Coin Ninja on or about July 13, 2017.

45. Neither Coin Ninja, nor its DropBit service, have ever registered as a money services business with FinCEN.

B. Failure to Establish Anti-Money Laundering Programs and Procedures

46. Under the Bank Secrecy Act, a money services business must develop, implement, and maintain an effective anti-money laundering program that is reasonably designed to prevent the money services business from being used to facilitate money laundering and the financing of terrorist activities. 31 U.S.C. §§ 5318(a)(2), (h); 31 C.F.R. § 1022.210(a).

47. An effective anti-money laundering program is one that is reasonably designed to prevent the money services business from being used to facilitate money laundering and the financing of terrorist activities. 31 C.F.R. § 1022.210(a). The anti-money laundering program must be commensurate with the risks posed by the location and size of, and the nature and volume of the financial services provided by the money services business, 31 C.F.R. § 1022.210(b), and it must: contain written policies, procedures and internal controls; designate an individual responsible for Bank Secrecy Act compliance; provide training, including on how to detect suspicious transactions; and provide for independent review of the anti-money laundering program. 31 U.S.C. §§ 5318(a)(2), (h); 31 C.F.R. §§ 1022.210(c), (d).

48. Harmon never implemented any type of anti-money laundering program related to Helix and failed to comply with all these requirements.

49. Harmon failed to establish and maintain appropriate internal controls to ensure compliance with the Bank Secrecy Act's reporting requirements during the operation of his business.

50. In fact, 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, 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.

51. Despite requiring account creation for transactions through Helix, Harmon chose not to collect information on any of the over 809,500 unique addresses sending and receiving bitcoin. In addition, Harmon also offered a service, Helix Light that allowed customers to conduct transactions without even creating the accounts.

52. As a result, 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. In fact, during its entire operational period, Harmon openly advertised Helix as a service that did not conduct customer due diligence.

53. During the operational period, Harmon conducted over \$311 million worth of transactions in convertible virtual currencies without performing appropriate due diligence on transactions or customers.

54. Harmon also failed to implement policies and procedures to file reports required by the Bank Secrecy Act and to create and retain appropriate records. Harmon asserted that he deleted any customer information Helix had after a period of seven days. Harmon also claimed to allow customers to delete their own customer information at will. Such a policy made it impossible for Harmon to comply with the requirements of the Bank Secrecy Act.

55. More specifically, 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.

56. Harmon also 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 financing.

57. A money services business is also required to designate a person to assure day to day compliance with their compliance program and the Bank Secrecy Act. 31 C.F.R. § 1022.210(d)(2)(i)–(iii). This person is responsible for assuring that the money services business files reports and creates and retains records, assuring that the compliance program is updated as necessary to reflect the current requirements of the Bank Secrecy Act, and providing appropriate training.

58. At no point in Helix’s operations did Harmon designate a person to assure day to day compliance with its compliance program and the Bank Secrecy Act.

59. A money services business must provide for training of personnel, including training in the detection of suspicious transactions. 31 C.F.R. § 1022.210(d)(3).

60. Harmon failed to train appropriate personnel in Bank Secrecy Act recordkeeping and reporting requirements and failed to train personnel in identifying, monitoring, and reporting suspicious activity.

61. A money services business must provide for independent review to monitor and maintain an adequate program. 31 C.F.R. § 1022.210(d)(4). At no point in its operations did Harmon conduct an independent test.

C. Failure to File Suspicious Activity Reports

62. Under the Bank Secrecy Act, a money services business must report transactions that the money services business “knows, suspects, or has reason to suspect” are suspicious where those transactions involve the money services business and aggregate to at least \$2,000 in value. 31 U.S.C. § 5318(g)(1); 31 C.F.R. § 1022.320(a)(2).

63. A transaction is “suspicious” if it (a) involves funds derived from illegal activity; (b) is designed to evade reporting requirements; (c) has no business or apparent lawful purpose; or (d) involves the use of the money services business to facilitate illegal activity. 31 U.S.C. § 5318(g)(1); 31 C.F.R. §§ 1022.320(a)(2)(i)–(iv).

64. Despite the rampant evidence of illegal activity on the platforms he operated, Harmon did not file a single Suspicious Activity Report, including for the specific activities identified in FinCEN’s Assessment. FinCEN specifically identified at least 2,464 instances in which Harmon failed to file a Suspicious Activity Report for transactions involving Helix.

65. On October 19, 2020, FinCEN assessed Harmon with a civil monetary penalty for the conduct described above.

66. To date, Harmon has not paid the assessed penalty.

COUNT I – RECOVERY OF CIVIL MONETARY PENALTY

67. The United States repeats and re-alleges the allegations contained in Paragraphs 1 to 66 above as if fully set forth herein.

68. The October 19, 2020, Assessment of Civil Money Penalty constitutes a lawful administrative sanction against Harmon for failure to comply with the Bank Secrecy Act’s requirements under 31 U.S.C. §§ 5321(b) and 5330(e).

69. Harmon is liable to the United States for a civil penalty plus interest and costs.

* * *

PRAYER FOR RELIEF

The United States respectfully requests that the Court reduce the civil penalty assessed by FinCEN against Harmon to judgment by awarding the United States a money judgment in an amount to be determined by the Court, plus interest as provided by law, and award such other relief as the Court deems just and proper.

Dated: October 19, 2022
Washington, DC

Respectfully submitted,

MATTHEW M. GRAVES, D.C. Bar #481052
United States Attorney

By: /s/ Brian P. Hudak
BRIAN P. HUDAK
Chief, Civil Division
601 D Street, NW
Washington, DC 20530
(202) 252-2549

Attorneys for the United States of America

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

IN THE MATTER OF:

**Larry Dean Harmon
d/b/a Helix**

Akron, Ohio

)
)
)
)
)
)
)
)
)

Number 2020-02

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

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).

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).

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).

³ 31 C.F.R. § 1010.810(a).

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.

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 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

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.

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.

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

IV. 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

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.

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:

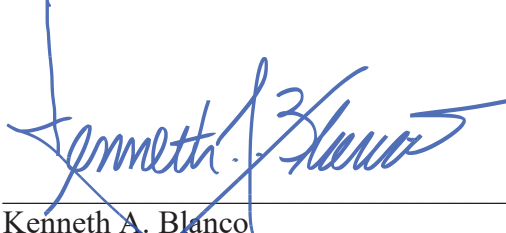
1. Nature and seriousness of the violations and harm to the public. The violations outlined in this ASSESSMENT are considered by FinCEN to be of a serious and egregious nature. The BSA and its implementing regulations require MSBs and money transmitters such as Helix to develop and implement a risk-based 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

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



Kenneth A. Blanco
Director
Financial Crimes Enforcement Network
U.S. Department of the Treasury
Date: 10.19.20

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).

Larry Dean Harmon d/b/a Helix

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 administering 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;

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

Larry Dean Harmon d/b/a Helix

- 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.
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

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.

Larry Dean Harmon d/b/a Helix

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

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

⁶ See Treasury Order 180-01 (July 1, 2014).

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).

Larry Dean Harmon d/b/a Helix

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.

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

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).

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_deanonimization_the_response/, December 7, 2014.

¹⁷ gramsadmin, “Helix : Agora bitcoin claim process?,” https://www.reddit.com/r/DarkNetMarkets/comments/2nanzl/helix_agora_bitcoin_claim_process/ Reddit, November 24, 2014.

Larry Dean Harmon d/b/a Helix

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. 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 delete 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

¹⁸ gramsadmin, “Helix : Agora bitcoin claim process?,” https://www.reddit.com/r/DarkNetMarkets/comments/2nanzl/helix_agora_bitcoin_claim_process/Reddit, November 24, 2014.

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.

Larry Dean Harmon d/b/a Helix

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.

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 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.

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).

Larry Dean Harmon d/b/a Helix

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. 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 31 C.F.R. § 1022.320.

²⁷ 31 C.F.R. §§ 1022.320(a)(2)(i) – (iv).

Larry Dean Harmon d/b/a Helix

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. **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

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.

Larry Dean Harmon d/b/a Helix

\$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

Larry Dean Harmon d/b/a Helix

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.

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.

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>.

Larry Dean Harmon d/b/a Helix

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.

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

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>.

Larry Dean Harmon d/b/a Helix

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.

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

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

50. **JoinMarket.** FinCEN observed Helix conducting 52 direct bitcoin transactions worth \$42,219 with the mixing service JoinMarket. At least seven of these direct transactions were for amounts over \$2,000. Mr. Harmon failed to file SARs 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>.

Larry Dean Harmon d/b/a Helix

51. **SharedCoin.** FinCEN observed Helix conducting 1,149 direct bitcoin transactions worth \$164,943 with the mixing service SharedCoin. 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.

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 as an 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

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>.

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.

Larry Dean Harmon d/b/a Helix

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.

CIVIL COVER SHEET

JS-44 (Rev. 11/2020 DC)

I. (a) PLAINTIFFS UNITED STATES OF AMERICA (b) COUNTY OF RESIDENCE OF FIRST LISTED PLAINTIFF (EXCEPT IN U.S. PLAINTIFF CASES)	DEFENDANTS LARRY DEAN HARMON (d/b/a Helix) COUNTY OF RESIDENCE OF FIRST LISTED DEFENDANT 88888 (IN U.S. PLAINTIFF CASES ONLY) <small>NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED</small>
(c) ATTORNEYS (FIRMNAME, ADDRESS, AND TELEPHONE NUMBER) Brian P. Hudak U.S. Attorney's Office for D.C., Civil Division 601 D Street, NW, Washington, DC 20530 (202) 252-2500	ATTORNEYS (IF KNOWN) Unknown

II. BASIS OF JURISDICTION (PLACE AN x IN ONE BOX ONLY) <div style="display: flex; justify-content: space-between;"> <div style="width: 48%;"> <input checked="" type="radio"/> 1 U.S. Government Plaintiff </div> <div style="width: 48%;"> <input type="radio"/> 3 Federal Question (U.S. Government Not a Party) </div> </div> <div style="display: flex; justify-content: space-between; margin-top: 10px;"> <div style="width: 48%;"> <input type="radio"/> 2 U.S. Government Defendant </div> <div style="width: 48%;"> <input type="radio"/> 4 Diversity (Indicate Citizenship of Parties in item III) </div> </div>	III. CITIZENSHIP OF PRINCIPAL PARTIES (PLACE AN x IN ONE BOX FOR PLAINTIFF AND ONE BOX FOR DEFENDANT) FOR DIVERSITY CASES ONLY! <table style="width: 100%; border: none;"> <thead> <tr> <th></th> <th style="text-align: center;">PTF</th> <th style="text-align: center;">DFT</th> <th></th> <th style="text-align: center;">PTF</th> <th style="text-align: center;">DFT</th> </tr> </thead> <tbody> <tr> <td>Citizen of this State</td> <td style="text-align: center;"><input type="radio"/> 1</td> <td style="text-align: center;"><input type="radio"/> 1</td> <td>Incorporated or Principal Place of Business in This State</td> <td style="text-align: center;"><input type="radio"/> 4</td> <td style="text-align: center;"><input type="radio"/> 4</td> </tr> <tr> <td>Citizen of Another State</td> <td style="text-align: center;"><input type="radio"/> 2</td> <td style="text-align: center;"><input type="radio"/> 2</td> <td>Incorporated and Principal Place of Business in Another State</td> <td style="text-align: center;"><input type="radio"/> 5</td> <td style="text-align: center;"><input type="radio"/> 5</td> </tr> <tr> <td>Citizen or Subject of a Foreign Country</td> <td style="text-align: center;"><input type="radio"/> 3</td> <td style="text-align: center;"><input type="radio"/> 3</td> <td>Foreign Nation</td> <td style="text-align: center;"><input type="radio"/> 6</td> <td style="text-align: center;"><input type="radio"/> 6</td> </tr> </tbody> </table>		PTF	DFT		PTF	DFT	Citizen of this State	<input type="radio"/> 1	<input type="radio"/> 1	Incorporated or Principal Place of Business in This State	<input type="radio"/> 4	<input type="radio"/> 4	Citizen of Another State	<input type="radio"/> 2	<input type="radio"/> 2	Incorporated and Principal Place of Business in Another State	<input type="radio"/> 5	<input type="radio"/> 5	Citizen or Subject of a Foreign Country	<input type="radio"/> 3	<input type="radio"/> 3	Foreign Nation	<input type="radio"/> 6	<input type="radio"/> 6
	PTF	DFT		PTF	DFT																				
Citizen of this State	<input type="radio"/> 1	<input type="radio"/> 1	Incorporated or Principal Place of Business in This State	<input type="radio"/> 4	<input type="radio"/> 4																				
Citizen of Another State	<input type="radio"/> 2	<input type="radio"/> 2	Incorporated and Principal Place of Business in Another State	<input type="radio"/> 5	<input type="radio"/> 5																				
Citizen or Subject of a Foreign Country	<input type="radio"/> 3	<input type="radio"/> 3	Foreign Nation	<input type="radio"/> 6	<input type="radio"/> 6																				

IV. CASE ASSIGNMENT AND NATURE OF SUIT

(Place an X in one category, A-N, that best represents your Cause of Action and one in a corresponding Nature of Suit)

<input type="radio"/> A. Antitrust <input type="checkbox"/> 410 Antitrust	<input type="radio"/> B. Personal Injury/Malpractice <input type="checkbox"/> 310 Airplane <input type="checkbox"/> 315 Airplane Product Liability <input type="checkbox"/> 320 Assault, Libel & Slander <input type="checkbox"/> 330 Federal Employers Liability <input type="checkbox"/> 340 Marine <input type="checkbox"/> 345 Marine Product Liability <input type="checkbox"/> 350 Motor Vehicle <input type="checkbox"/> 355 Motor Vehicle Product Liability <input type="checkbox"/> 360 Other Personal Injury <input type="checkbox"/> 362 Medical Malpractice <input type="checkbox"/> 365 Product Liability <input type="checkbox"/> 367 Health Care/Pharmaceutical Personal Injury Product Liability <input type="checkbox"/> 368 Asbestos Product Liability	<input type="radio"/> C. Administrative Agency Review <input type="checkbox"/> 151 Medicare Act <u>Social Security</u> <input type="checkbox"/> 861 HIA (1395ff) <input type="checkbox"/> 862 Black Lung (923) <input type="checkbox"/> 863 DIWC/DIWW (405(g)) <input type="checkbox"/> 864 SSID Title XVI <input type="checkbox"/> 865 RSI (405(g)) <u>Other Statutes</u> <input type="checkbox"/> 891 Agricultural Acts <input type="checkbox"/> 893 Environmental Matters <input type="checkbox"/> 890 Other Statutory Actions (If Administrative Agency is Involved)	<input type="radio"/> D. Temporary Restraining Order/Preliminary Injunction Any nature of suit from any category may be selected for this category of case assignment. *(If Antitrust, then A governs)*
---	--	--	--

<input checked="" type="radio"/> E. General Civil (Other)	<input type="radio"/> F. Pro Se General Civil
--	--

<u>Real Property</u> <input type="checkbox"/> 210 Land Condemnation <input type="checkbox"/> 220 Foreclosure <input type="checkbox"/> 230 Rent, Lease & Ejectment <input type="checkbox"/> 240 Torts to Land <input type="checkbox"/> 245 Tort Product Liability <input type="checkbox"/> 290 All Other Real Property <u>Personal Property</u> <input type="checkbox"/> 370 Other Fraud <input type="checkbox"/> 371 Truth in Lending <input type="checkbox"/> 380 Other Personal Property Damage <input type="checkbox"/> 385 Property Damage Product Liability	<u>Bankruptcy</u> <input type="checkbox"/> 422 Appeal 27 USC 158 <input type="checkbox"/> 423 Withdrawal 28 USC 157 <u>Prisoner Petitions</u> <input type="checkbox"/> 535 Death Penalty <input type="checkbox"/> 540 Mandamus & Other <input type="checkbox"/> 550 Civil Rights <input type="checkbox"/> 555 Prison Conditions <input type="checkbox"/> 560 Civil Detainee – Conditions of Confinement <u>Property Rights</u> <input type="checkbox"/> 820 Copyrights <input type="checkbox"/> 830 Patent <input type="checkbox"/> 835 Patent – Abbreviated New Drug Application <input type="checkbox"/> 840 Trademark <input type="checkbox"/> 880 Defend Trade Secrets Act of 2016 (DTSA)	<u>Federal Tax Suits</u> <input type="checkbox"/> 870 Taxes (US plaintiff or defendant) <input type="checkbox"/> 871 IRS-Third Party 26 USC 7609 <u>Forfeiture/Penalty</u> <input type="checkbox"/> 625 Drug Related Seizure of Property 21 USC 881 <input type="checkbox"/> 690 Other <u>Other Statutes</u> <input type="checkbox"/> 375 False Claims Act <input type="checkbox"/> 376 Qui Tam (31 USC 3729(a)) <input type="checkbox"/> 400 State Reapportionment <input checked="" type="checkbox"/> 430 Banks & Banking <input type="checkbox"/> 450 Commerce/ICC Rates/etc <input type="checkbox"/> 460 Deportation <input type="checkbox"/> 462 Naturalization Application	<input type="checkbox"/> 465 Other Immigration Actions <input type="checkbox"/> 470 Racketeer Influenced & Corrupt Organization <input type="checkbox"/> 480 Consumer Credit <input type="checkbox"/> 485 Telephone Consumer Protection Act (TCPA) <input type="checkbox"/> 490 Cable/Satellite TV <input type="checkbox"/> 850 Securities/Commodities/Exchange <input type="checkbox"/> 896 Arbitration <input type="checkbox"/> 899 Administrative Procedure Act/Review or Appeal of Agency Decision <input type="checkbox"/> 950 Constitutionality of State Statutes <input type="checkbox"/> 890 Other Statutory Actions (if not administrative agency review or Privacy Act)
---	---	---	--

<input type="radio"/> G. Habeas Corpus/ 2255 <input type="checkbox"/> 530 Habeas Corpus – General <input type="checkbox"/> 510 Motion/Vacate Sentence <input type="checkbox"/> 463 Habeas Corpus – Alien Detainee	<input type="radio"/> H. Employment Discrimination <input type="checkbox"/> 442 Civil Rights – Employment (criteria: race, gender/sex, national origin, discrimination, disability, age, religion, retaliation) *(If pro se, select this deck)*	<input type="radio"/> I. FOIA/Privacy Act <input type="checkbox"/> 895 Freedom of Information Act <input type="checkbox"/> 890 Other Statutory Actions (if Privacy Act) *(If pro se, select this deck)*	<input type="radio"/> J. Student Loan <input type="checkbox"/> 152 Recovery of Defaulted Student Loan (excluding veterans)
<input type="radio"/> K. Labor/ERISA (non-employment) <input type="checkbox"/> 710 Fair Labor Standards Act <input type="checkbox"/> 720 Labor/Mgmt. Relations <input type="checkbox"/> 740 Labor Railway Act <input type="checkbox"/> 751 Family and Medical Leave Act <input type="checkbox"/> 790 Other Labor Litigation <input type="checkbox"/> 791 Empl. Ret. Inc. Security Act	<input type="radio"/> L. Other Civil Rights (non-employment) <input type="checkbox"/> 441 Voting (if not Voting Rights Act) <input type="checkbox"/> 443 Housing/Accommodations <input type="checkbox"/> 440 Other Civil Rights <input type="checkbox"/> 445 Americans w/Disabilities – Employment <input type="checkbox"/> 446 Americans w/Disabilities – Other <input type="checkbox"/> 448 Education	<input type="radio"/> M. Contract <input type="checkbox"/> 110 Insurance <input type="checkbox"/> 120 Marine <input type="checkbox"/> 130 Miller Act <input type="checkbox"/> 140 Negotiable Instrument <input type="checkbox"/> 150 Recovery of Overpayment & Enforcement of Judgment <input type="checkbox"/> 153 Recovery of Overpayment of Veteran's Benefits <input type="checkbox"/> 160 Stockholder's Suits <input type="checkbox"/> 190 Other Contracts <input type="checkbox"/> 195 Contract Product Liability <input type="checkbox"/> 196 Franchise	<input type="radio"/> N. Three-Judge Court <input type="checkbox"/> 441 Civil Rights – Voting (if Voting Rights Act)

V. ORIGIN
☒ 1 Original Proceeding
 ☐ 2 Removed from State Court
 ☐ 3 Remanded from Appellate Court
 ☐ 4 Reinstated or Reopened
 ☐ 5 Transferred from another district (specify)
 ☐ 6 Multi-district Litigation
 ☐ 7 Appeal to District Judge from Mag. Judge
 ☐ 8 Multi-district Litigation – Direct File

VI. CAUSE OF ACTION (CITE THE U.S. CIVIL STATUTE UNDER WHICH YOU ARE FILING AND WRITE A BRIEF STATEMENT OF CAUSE.)
 31 U.S.C. §§ 5321 - Suit to reduce assessed Bank Secrecy Act civil penalty to judgment

VII. REQUESTED IN COMPLAINT

☐ CHECK IF THIS IS A CLASS ACTION UNDER F.R.C.P. 23

DEMAND \$ TBD
JURY DEMAND:

Check YES only if demanded in complaint
 YES ☐ NO ☒

VIII. RELATED CASE(S) IF ANY

(See instruction)

YES ☒ NO ☐

If yes, please complete related case form

DATE: 10/19/2022

SIGNATURE OF ATTORNEY OF RECORD /s/ Brian P. Hudak

INSTRUCTIONS FOR COMPLETING CIVIL COVER SHEET JS-44
 Authority for Civil Cover Sheet

The JS-44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and services of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. Listed below are tips for completing the civil coversheet. These tips coincide with the Roman Numerals on the cover sheet.

- I.** COUNTY OF RESIDENCE OF FIRST LISTED PLAINTIFF/DEFENDANT (b) County of residence: Use 11001 to indicate plaintiff if resident of Washington, DC, 88888 if plaintiff is resident of United States but not Washington, DC, and 99999 if plaintiff is outside the United States.
- III.** CITIZENSHIP OF PRINCIPAL PARTIES: This section is completed only if diversity of citizenship was selected as the Basis of Jurisdiction under Section II.
- IV.** CASE ASSIGNMENT AND NATURE OF SUIT: The assignment of a judge to your case will depend on the category you select that best represents the primary cause of action found in your complaint. You may select only one category. You must also select one corresponding nature of suit found under the category of the case.
- VI.** CAUSE OF ACTION: Cite the U.S. Civil Statute under which you are filing and write a brief statement of the primary cause.
- VIII.** RELATED CASE(S), IF ANY: If you indicated that there is a related case, you must complete a related case form, which may be obtained from the Clerk's Office.

Because of the need for accurate and complete information, you should ensure the accuracy of the information provided prior to signing the form.

CLERK'S OFFICE
UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

CO-932
Rev. 4/96

NOTICE OF DESIGNATION OF RELATED CIVIL CASES PENDING
IN THIS OR ANY OTHER UNITED STATES COURT

Civil Action No. 22-3203
(To be supplied by the Clerk)

NOTICE TO PARTIES:

Pursuant to Rule 40.5(b)(2), you are required to prepare and submit this form at the time of filing any civil action which is related to any pending cases or which involves the same parties and relates to the same subject matter of any dismissed related cases. This form must be prepared in sufficient quantity to provide one copy for the Clerk's records, one copy for the Judge to whom the cases is assigned and one copy for each defendant, so that you must prepare 3 copies for a one defendant case, 4 copies for a two defendant case, etc.

NOTICE TO DEFENDANT:

Rule 40.5(b)(2) of this Court requires that you serve upon the plaintiff and file with your first responsive pleading or motion any objection you have to the related case designation.

NOTICE TO ALL COUNSEL

Rule 40.5(b)(3) of this Court requires that as soon as an attorney for a party becomes aware of the existence of a related case or cases, such attorney shall immediately notify, in writing, the Judges on whose calendars the cases appear and shall serve such notice on counsel for all other parties.

The plaintiff, defendant or counsel must complete the following:

I. RELATIONSHIP OF NEW CASE TO PENDING RELATED CASE(S).

A new case is deemed related to a case pending in this or another U.S. Court if the new case: [Check appropriate box(e's) below.]

- ☐ (a) relates to common property
- ☒ (b) involves common issues of fact
- ☒ (c) grows out of the same event or transaction
- ☐ (d) involves the validity or infringement of the same patent
- ☐ (e) is filed by the same pro se litigant

2. RELATIONSHIP OF NEW CASE TO DISMISSED RELATED CASE(ES)

A new case is deemed related to a case dismissed, with or without prejudice, in this or any other U.S. Court, if the new case involves the same parties and same subject matter.

Check box if new case is related to a dismissed case: ☐

3. NAME THE UNITED STATES COURT IN WHICH THE RELATED CASE IS FILED (IF OTHER THAN THIS COURT):

N/A

4. CAPTION AND CASE NUMBER OF RELATED CASE(E'S). IF MORE ROOM IS NEED PLEASE USE OTHER SIDE.

UNITED STATES v. HARMON, Crim. No. 19-0395 (BAH) C.A. No. _____

10/19/2022
DATE

/s/ Brian P. Hudak, Civil Chief, U.S. Attorney's Office
Signature of Plaintiff/Defendant (or counsel)

UNITED STATES DISTRICT COURT

for the

District of Columbia



UNITED STATES OF AMERICA

Plaintiff(s)

v.

LARRY DEAN HARMON (d/b/a Helix)

Defendant(s)

Civil Action No. 22-3203

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)* LARRY DEAN HARMON (d/b/a Helix)
 3853 Yellow Creek Rd.
 Akron, OH 44333

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are:

Brian P. Hudak
 U.S. Attorney's Office for D.C.
 Civil Division
 601 D Street, NW
 Washington, DC 20530

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

ANGELA D. CAESAR, CLERK OF COURT

Date: _____

Signature of Clerk or Deputy Clerk

Civil Action No. 22-3203

PROOF OF SERVICE*(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))*

This summons for *(name of individual and title, if any)* _____
 was received by me on *(date)* _____.

☐ I personally served the summons on the individual at *(place)* _____
 _____ on *(date)* _____; or

☐ I left the summons at the individual's residence or usual place of abode with *(name)* _____
 _____, a person of suitable age and discretion who resides there,
 on *(date)* _____, and mailed a copy to the individual's last known address; or

☐ I served the summons on *(name of individual)* _____, who is
 designated by law to accept service of process on behalf of *(name of organization)* _____
 _____ on *(date)* _____; or

☐ I returned the summons unexecuted because _____; or

☐ Other *(specify)*:

My fees are \$ _____ for travel and \$ _____ for services, for a total of \$ 0.00.

I declare under penalty of perjury that this information is true.

Date: _____

Server's signature

Printed name and title

Server's address

Additional information regarding attempted service, etc: