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 administrating 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