

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

COMMODITY FUTURES TRADING
COMMISSION,

Plaintiff,

v.

OR PATREANU, SNIR HANANYA, ARTEM
PROKOPENKO, ELIJAH SAMSON, and
EXPECTED VALUE PLUS LTD.,

Defendants.

Case No. 23-cv-20782

ECF Case

**COMPLAINT FOR INJUNCTIVE
AND OTHER EQUITABLE RELIEF
AND FOR CIVIL MONETARY
PENALTIES UNDER THE
COMMODITY EXCHANGE ACT
AND COMMISSION REGULATIONS**

JURY TRIAL DEMANDED

Commodity Futures Trading
Commission, Plaintiff
290 Broadway
New York, NY 10007

John C. Murphy
Trial Attorney
jmurphy@cftc.gov
Phone: (646) 746-9700

K. Brent Tomer
Chief Trial Attorney
ktomer@cftc.gov
Phone: (646) 746-9700

Manal M. Sultan
Deputy Director
msultan@cftc.gov
Phone: (646) 746-9700

Or Patreanu, Defendant
Last Known Address:
Beit Horon 3 Tel Aviv
Motifyory 3/1
Tel Aviv, Israel

Snir Hananya, Defendant
Last Known Address:
Via Gennargentu 2
09170 Oristano OR, Italy

Artem Prokopenko, Defendant
Last Known Address:
Kurguzova 3B, Apt 14
Vishgorod, Ukraine

Elijah Samson, Defendant
Last Known Address:
Mittelstr. 21B
13055 Berlin, Germany

Expected Value Plus, Ltd.
Suite 108, Premier Building
Victoria, Mahe, Seychelles

I. INTRODUCTION

1. From at least in or around January 1, 2017 through at least October 2021 (the “Relevant Period”), Defendants Or Patreanu, Snir Hananya, Artem Prokopenko, Elijah Samson, and Expected Value Plus Ltd. (collectively, “Defendants”), doing business under multiple brand names including Trade2Get, Coinbull, Cryptonxt, Tradenix, Cryptobravos, Nittrex, Wobit, and Pinance (collectively, “Cryptobravos”), operated a fraudulent scheme in which they solicited bitcoin and other funds from members of the public (“customers”), in the United States and abroad, for the stated purpose of establishing managed accounts for the purchase, sale, and trading of digital asset commodities, including virtual currencies such as bitcoin, a commodity in interstate commerce. In truth, Defendants (and Cryptobravos as a whole) conducted little or no trading on behalf of its customers; instead, Defendants simply accepted customers’ funds and refused to return them, often after encouraging customers to empty their retirement accounts or take out loans for the purpose of making additional deposits. During the Relevant Period, Defendants obtained bitcoin and other funds worth tens of millions of dollars from hundreds of customers through fraudulent solicitations. Defendants misappropriated, either directly or indirectly, substantially all of the bitcoin and other funds they received from customers during the Relevant Period.

2. Cryptobravos employed dozens of persons in call centers in Tel Aviv, Israel; Kiev, Ukraine; Kharkov, Ukraine; Tirana, Albania; and Johannesburg, South Africa, among other locations, and operated through a network of front companies. Patreanu, Hananya, and Prokopenko (together, the “Controlling Defendants”) collectively managed these calls centers and front companies as a common enterprise and controlled every aspect of Cryptobravos, including its finances, operations, and employees. Samson was a high-level call center

employee, and in that capacity, he fraudulently solicited over 130 bitcoin with a present value of over \$3 million, as well as over \$400,000 in fiat currency.

3. In furtherance of the fraudulent scheme, Defendants (as well as dozens of other Cryptobravos agents and employees under the control of Patreanu, Hananya, and Prokopenko) made countless fraudulent misrepresentations of material facts in solicitations to actual and prospective customers, including representations that: (a) Cryptobravos had offices in New York; (b) Cryptobravos would trade and trade customers' assets; (c) customers would earn risk-free profits; (d) customers had earned substantial profits; and (e) customers could withdraw their funds at any time. Defendants also failed to disclose countless material facts, including that Defendants misappropriated and intended to misappropriate virtually all of its customers' funds.

4. Through this conduct, Defendants have engaged, are engaging, or are about to engage in fraudulent acts and practices in violation of the Commodity Exchange Act ("Act"), 7 U.S.C. §§ 1–26, and Commission Regulations ("Regulations"), 17 C.F.R. pts. 1–190 (2022), specifically Section 6(c)(1) of the Act, 7 U.S.C. § 9(1), and Regulation 180.1(a)(1)-(3), 17 C.F.R. § 180.1(a)(1)-(3) (2022).

5. In addition to being primarily liable for Cryptobravos's acts and practices, Patreanu, Hananya, and Prokopenko were also controlling persons of Cryptobravos. The Controlling Defendants did not act in good faith and knowingly induced Cryptobravos's and its employees' and agents' violations of the Act and Regulations described herein during the Relevant Period. Therefore, the Controlling Defendants are liable for Cryptobravos's violations of the Act and Regulations pursuant to Section 13(b) of the Act, 7 U.S.C. § 13c(b). The Controlling Defendants also aided and abetted Samson's and other Cryptobravos agents' and

employees' violations and are therefore also liable for those violations pursuant to Section 13(a) of the Act, 7 U.S.C. § 13c(a).

6. Accordingly, pursuant to Section 6c of the Act, 7 U.S.C. § 13a-1, the Commission brings this action to enjoin such acts and practices and compel compliance with the Act. In addition, the Commission seeks civil monetary penalties and remedial ancillary relief, including but not limited to trading bans, restitution, disgorgement, rescission, pre- and post-judgment interest, and such other relief as the Court may deem necessary and appropriate.

7. Unless restrained and enjoined by this Court, Defendant is likely to continue to engage in the acts and practices alleged in this Complaint and similar acts and practices, as more fully described below.

II. JURISDICTION AND VENUE

8. **Jurisdiction.** This Court has jurisdiction over this action under 28 U.S.C. § 1331 (federal question jurisdiction) and 28 U.S.C. § 1345 (district courts have original jurisdiction over civil actions commenced by the United States or by any agency expressly authorized to sue by Act of Congress). In addition, Section 6c(a) of the Act, 7 U.S.C. § 13a-1(a), authorizes the Commission to seek injunctive and other relief against any person whenever it appears to the Commission that such person has engaged, is engaging, or is about to engage in any act or practice constituting a violation of any provision of the Act or any rule, regulation, or order thereunder.

9. **Venue.** Venue properly lies with the Court pursuant to Section 6c(e) of the Act, 7 U.S.C. § 13a-1(e), because Defendants transacted business in this District, and because acts and practices in violation of the Act occurred, are occurring, or are about to occur, within this

District. Among other things, Defendants solicited customers located in this district and accepted deposits from customers located in this district.

III. THE PARTIES

10. Plaintiff **Commodity Futures Trading Commission** (“Commission” or “CFTC”) is an independent federal regulatory agency that is charged by Congress with the administration and enforcement of the Act and the Regulations. The Commission maintains its principal office at Three Lafayette Centre, 1155 21st Street, N.W. Washington, D.C. 20581 and its Eastern Regional Office at 290 Broadway, New York, NY 10007.

11. Defendant **Or Patreanu** is a natural person with a last known residence in Tel Aviv, Israel. Patreanu has never been registered with the Commission.

12. Defendant **Snir Hananya** is a natural person with a last known residence in Italy. Hananya has never been registered with the Commission.

13. Defendant **Artem Prokopenko** is a natural person with a last known residence in Kiev, Ukraine. Prokopenko has never been registered with the Commission.

14. Defendant **Elijah Samson** is a natural person with a last known residence in Germany. Samson has never been registered with the Commission.

15. Defendant **Expected Value Plus Ltd.** is a Seychelles company wholly owned and controlled by Patreanu and Hananya. Expected Value Plus has never been registered with the Commission.

IV. FACTS

16. A virtual currency is a type of digital asset commodity defined here as a digital representation of value that functions as a medium of exchange, a unit of account, and/or a store

of value. Bitcoin and certain other virtual currencies are commodities as defined under Section 1a(9) of the Act, 7 U.S.C. § 1a(9).

17. During the Relevant Period, Defendants solicited and received virtual currency then equivalent to tens of millions of dollars from hundreds of customers, who deposited amounts ranging from a few hundred dollars to hundreds of thousands of dollars, in both fiat currency and virtual currency, for the purpose of entering into contracts of sale of virtual currency commodities in interstate commerce.

A. Cryptobravos's Structure and Operation

18. Defendants' aim was to solicit deposits from customers in the United States and around the world through fraud. Under the direction and control of the Controlling Defendants, Cryptobravos's agents and employees, including Samson, represented to customers that Cryptobravos would execute virtual currency trades in managed accounts on its customers' behalf and allow customers to participate in supposedly exclusive and risk-free virtual currency purchase opportunities. In reality, Defendants made few if any trades for its customers, and the purchase opportunities were fake. Defendants simply took their customers' deposits and refused to return them when asked.

19. Patreanu and Hananya began doing business under the brand name Trade2Get in or around early 2017. Between 2017 and 2022, Cryptobravos changed brand names frequently in order to evade regulatory and criminal scrutiny and to minimize online negative reviews. During the Relevant Period, Defendants conducted business under the brand names Trade2Get, Coinbull, Cryptonxt, Tradenix, Cryptobravos, Nittrex, Pinance, and Wobit. These brand names, along with the front companies that ran them, were operated as a common enterprise and are collectively referred to herein as "Cryptobravos."

20. Cryptobravos told customers it was based in New York, Chicago, London, Zurich, or other international business centers. In truth, Cryptobravos had no offices in these locations. Instead, Cryptobravos maintained offices in Tel Aviv, Israel; Kiev, Ukraine; Kharkov, Ukraine; Tirana, Albania; and Johannesburg, South Africa, among other locations.

21. Each Cryptobravos office housed a call center, and Cryptobravos as a whole employed dozens of individuals who staffed the phones and communicated with customers by telephone and email, under the direction and control of the Controlling Defendants. Phone calls from Cryptobravos's call centers targeted and reached United States customers and were made to appear as if they originated from United States locations, including New York. In order to conceal their true identities and evade regulatory and criminal scrutiny, Cryptobravos's management (including Patreanu, Hananya, and Prokopenko) and agents and employees (including Samson) used a variety of fake names and pseudonyms, referred to internally as "stage names." Employees changed stage names frequently, typically coinciding with Cryptobravos's changes in public-facing brand names. But while stage names and brand names changed over time, Patreanu's, Hananya's, and Prokopenko's control over the fraudulent scheme remained constant. Together, Patreanu, Hananya, and Prokopenko oversaw and controlled all aspects of Cryptobravos.

22. Patreanu functioned as Cryptobravos's co-CEO. He personally managed the Tel Aviv office, which he visited at least once per week. Using the pseudonym "Manager1," Patreanu maintained email addresses affiliated with multiple Cryptobravos brand names, including Coinbull and Tradenix. When dealing with Cryptobravos employees, Patreanu used a fake name, David Shapiro. During the Relevant Period, Patreanu managed Cryptobravos's finances and expenses; oversaw Cryptobravos's receipt of tens of millions of dollars of customer

funds; oversaw marketing and the generation of leads for Cryptobravos's customer solicitations; negotiated and determined salaries and commissions for Cryptobravos's Tel Aviv employees; disseminated and reviewed scripts for customer calls; and served as shareholder and director of Expected Value Plus Ltd., Cryptobravos's primary operating company. Patreanu was immersed in the details of Cryptobravos, and among other things, selected the logo for the Coinbull website and Facebook page; corresponded with real estate brokers regarding office space; corresponded with Expected Value Plus's banks to make payments relating to Coinbull and other brand names; approved individual wires from customers to certain bank accounts controlled by Cryptobravos; received daily and real-time updates regarding customer deposits; received and forwarded files containing tens of thousands of customer leads and sent those files to call centers; received periodic reports regarding the daily number and duration of calls made to customers by Cryptobravos employees; and received recordings of notable customer calls.

23. Hananya, along with Patreanu, functioned as Cryptobravos's co-CEO. Using the pseudonyms "M.services," and "Richard Goldsmith," Hananya maintained email addresses affiliated with multiple Cryptobravos brand names, including Trade2Get, Coinbull, Tradenix, and Cryptobravos. During the Relevant Period, Hananya managed Cryptobravos's finances and expenses; oversaw marketing and the generation of leads for customer solicitations; facilitated the creation of the front company that operated Cryptobravos's Ukrainian call centers; and served as the Director of Telemarketing for Cryptobravos's Albanian call center. Like Patreanu, Hananya was immersed in the details of Cryptobravos. Among other things, Hananya received and forwarded files containing tens of thousands of customer leads; received daily reports of new customers and deposits; determined and managed salary and bonus structure for employees of the Ukrainian call centers; supervised the opening of the Kiev call center in person during the

first few months of its operation; interviewed employees for positions at the Kiev call center; and managed the start of new “campaigns” to generate new customer deposits.

24. Prokopenko joined Cryptobravos in or around early 2017 and functioned as its chief operating officer, reporting to Patreanu and Hananya. Using the pseudonym “super user,” Prokopenko maintained email addresses affiliated with multiple Cryptobravos brand names, including Coinbull, Tradenix, Cryptobravos, and Nittrex. During the Relevant Period, Prokopenko managed Cryptobravos’s information technology infrastructure, including telephones, databases, software, and websites; managed the finances and expenses of certain of Cryptobravos’s many front companies; and managed and oversaw Cryptobravos’s Ukrainian call centers. Prokopenko was immersed in the details of Cryptobravos. Among other things, Prokopenko received files containing tens of thousands of customer leads; received daily and real-time reports of new deposits; disseminated information to employees regarding available bank accounts to receive customer deposits; addressed specific IT issues relating to the functionality of Cryptobravos’s websites; and interviewed employees for positions at the Kiev call center.

25. Samson began working for Cryptobravos in 2018. During the Relevant Period, Samson served as an account manager and retention agent for Cryptobravos in the Kharkov call center and reported directly to Patreanu. In this capacity, Samson spoke directly to customers of Cryptobravos and knowingly made countless false and misleading statements and omissions of material fact for the purpose of soliciting deposits. When speaking with customers, Samson used the stage names “Daniel Grant” (Cryptonxt), “Steven Grant” (Tradenix), “Robert Ross” (Cryptobravos), “Paul Simmons” (Wobit), and “James Gold” (Pinance).

26. The Controlling Defendants operated Cryptobravos through a web of front companies. At the center was Expected Value Plus Ltd. (“Expected Value Plus”), a Seychelles company wholly owned and controlled by Patreanu and Hananya. Patreanu and Hananya were the sole shareholders of Expected Value Plus, and each served as its sole director at times during the Relevant Period. Patreanu and Hananya opened and controlled bank accounts in the name of Expected Value Plus. Through those accounts, Patreanu and Hananya received and disbursed funds to Cryptobravos’s many other front companies and received payment for the sale of bitcoin that Cryptobravos had stolen from its customers.

27. The Albanian and South African call centers were operated by NEK Marketing sh.p.k, (“NEK Marketing”) an Albanian company, and AV Group Investments (PTY) LTD (“AV Group”), a South African company, respectively. Both companies were controlled by Patreanu, Hananya, and Prokopenko. In correspondence with Bank 1, Expected Value Plus acknowledged that NEK Marketing and AV Group served as operating companies under Expected Value Plus. The same correspondence also attached, among other things, photos of NEK Marketing and AV Group offices, pay slips for employees of NEK Marketing and AV Group, and tenancy agreements for the offices of NEK Marketing and AV Group Investments, demonstrating Expected Value Plus’s (and Patreanu and Hananya’s) complete control over those companies. Prokopenko oversaw AV Group’s and NEK Marketing’s payroll. In addition, Prokopenko oversaw NEK Marketing’s budget and appointed its administrator (through Prokopenko’s control over NEK Marketing’s parent company, Best Media Ltd.).

28. Materials provided by Defendants to customers represented that the Cryptobravos and Cryptonxt brands were “divisions of” or “owned and operated by” Best Media Ltd. (“Best Media”), a Bulgarian Company. Best Media was controlled by Patreanu, Hananya, and

Prokopenko. Prokopenko opened accounts with payment services providers in the name of Best Media, managed payments to and from those accounts, and forwarded Best Media transaction records to Patreanu and Hananya. Accounts opened with payment services providers in the name of Best Media received deposits from Cryptobravos customers, and Prokopenko communicated with Patreanu and Hananya regarding those deposits and the balances in those accounts. Prokopenko also maintained logins and passwords for Best Media's accounts and shared them with Hananya. Patreanu had access to a credit card opened in the name of Best Media and used it for expenses, including paying for a flight to Albania. NEK Marketing was a wholly owned subsidiary of Best Media.

29. The Cryptobravos brand's website stated it was affiliated with a company called ABC Marketing Limited ("ABC Marketing"), based in the Commonwealth of Dominica. ABC Marketing was controlled by Patreanu, Hananya, and Prokopenko. Patreanu, Hananya, and Prokopenko opened accounts with payment services providers in the name of ABC Marketing. Prokopenko managed payments to and from those accounts and forwarded ABC Marketing transaction records to Patreanu. Patreanu also received certain transaction records for ABC Marketing directly from payment services providers. Prokopenko copied Hananya and Patreanu on certain communications with ABC Marketing's payment services providers and forwarded other communications relating to ABC Marketing's accounts to Patreanu and Hananya. Prokopenko also maintained logins and passwords for ABC Marketing's accounts and shared them with Hananya.

B. Defendants' False and Misleading Solicitations

30. Defendants' solicitations were rife with fraud, lies, and deceit. Each brand name had a unique website that was accessible in the United States, and virtually every aspect of those

websites was false or misleading. The Cryptobravos brand's website, for example, falsely claimed that the company had an office in Chicago. It claimed to give customers the opportunity to "Make money" by "Buy[ing] and Sell[ing] crypto currencies" and represented that customers "can withdraw money any time [they] want." These representations were false and misleading because Cryptobravos conducted little or no actual trading, its customers never received profits, and Defendants routinely refused requests for withdrawals and misappropriated customers' funds.

31. Customers could and did log into these websites, including from the United States (and this judicial district), with a username and password and view the purported transaction history and balance of their accounts. Samson and other Cryptobravos employees, under the direction and control of the Controlling Defendants, made false and misleading changes to customers' online transaction histories and account balances as it suited them. Customers' online transaction history typically reflected the trades and transactions that Cryptobravos claimed it had executed on its customers' behalf. Customers' account balances likewise typically reflected highly successful trading and substantial gains. These representations were false and misleading because Cryptobravos conducted little or no actual trading and earned no profits on its customers' behalf and earned no profits. In addition, Cryptobravos did not actually create segregated customer accounts. Instead, all funds received from customers were commingled and funneled to virtual currency wallets and companies controlled by Patreanu, Hananya, and Prokopenko.

32. With each customer, Defendants' fraud followed a typical path, with the goal of building trust and then stealing as much money as possible. Call center employees were trained to build rapport and confidence while harvesting details about customer finances that could be

exploited later. For example, a call script circulated by Patreanu to Cryptobravos employees in January 2018, for the purpose of dictating the substance of initial customer calls, contained the following instructions:

- “Grab his attention.”
- “[M]ake him feel comfortable. . . .
- “[B]uild him a business plan and understand where does he keep his money. . . . *get his financial picture *build him a plan with hope *give him close and far goals.”
- “Once you fell [sic] that you have enough Financial information on the client you move in for the Kill!”

33. Virtually nothing that Cryptobravos told its customers, from beginning to end, was true. Call center employees began by lying about their names and locations, and the lies grew from there. Patreanu’s call script likewise contained numerous misrepresentations. For example, his script instructed employees to make the following representation:

As your broker I get 3% commission every time we win a trade. When we lose the trade I lose my commission as well. So basically we are on the same boat, when you make money I make money, that simple, make sense?!?

This statement was false and misleading because Cryptobravos conducted little or no trading on behalf of its customers, and its employees were compensated based on the value of customer deposits, not profits from (non-existent) trading.

34. Patreanu’s call script further instructed call center employees to sell “risk-free” contracts that would yield an 80% return. The script described these contracts as follows:

What is a contract: We have a team of 12 Analysts – they analyze the Market 24/7. Now, only when 12 out of 12 say it’s a go, the CEO himself go and by [sic] those contracts directly from the Market.

These statements were false and misleading because, among other reasons, Cryptobravos did not have a team of analysts; Defendants did not intend to place customer funds into any contracts, and therefore customers would not receive an 80% return; and it omitted the material fact that Defendants intended to misappropriate customer funds.

35. Patreanu sent another call script to Prokopenko on December 26, 2017. This script instructed Cryptobravos employees to tell customers, among other things, that “we have investors that made well over 900% in the last year alone.” This statement was false and misleading because Cryptobravos did not trade its customers’ funds and omitted, among other things, the material facts that Cryptobravos would not allow withdrawals and intended to misappropriate customer funds. As a result, none of Cryptobravos’s customers received any profits, let alone profits on the order of 900%.

36. Defendants typically solicited small deposits from customers at first, in the range of hundreds of dollars, and promised that these deposits would be actively managed. After receiving an initial deposit, Defendants informed customers that they had executed trades on the customer’s behalf, and that those trades had been profitable. Occasionally, customers were allowed to make small withdrawals, in amounts far less than their total deposits, to give customers false confidence that their money was within reach. Then, leveraging the apparent “success” of the smaller trades, Defendants solicited larger and larger deposits from customers under the guise of various exclusive trading opportunities. Defendants encouraged customers to empty their retirement accounts, mortgage their homes, and take out personal and private loans for the purpose of raising more money to deposit.

37. **Customer 1**. On or around July 22, 2019, Samson emailed Patreanu a “Retention Report for New Leads,” which stated that Customer 1, a United States customer, had “Deposited

1k on first call.” On or around August 14, 2019, Customer 1 deposited an additional \$500 through a transfer from Exchange 1, a virtual currency exchange located in New York. On the same day, Samson reported the deposit to Patreanu along with the wallet address to which the deposit was sent. On October 21, 2019, Customer 1 sent another \$500 deposit to Cryptobravos through Exchange 1, and Samson wrote to Customer 1, “your account is growing good.” This representation was false and misleading because Samson had conducted no trades on Customer 1’s behalf.

38. On November 1, 2019, Samson emailed several customers, including Customer 1, regarding a “BITCOIN CHRISTMAS DAY GIVEAWAY” promotion. In the email, Samson wrote:

[O]ur Firm has increased the Profits by 75% in the last earnings report, due to that we have increased our mining servers which tripled the amount of Bitcoin’s [sic] mined by the Firm. Our Firm currently Mining Bitcoins [sic] with a HASH rate of 10 Million TH/s (Tera HASHes per Second) which generates above 65,000 BTCs per month. On this occasion, we offer our clients for the Month of November 2019 to prepare for their Christmas Holiday with their Families and Friends by investing in Bitcoins and Earning 100%. . . . The Offer and Conditions are as follows You invest a minimum of 1 Bitcoin and you will receive 100% from us, which means 1 Bitcoin. The Bitcoins you will be investing with the bonus you are receiving on them will be available to withdraw from 1st December 2019.

This solicitation was false and misleading because, among other reasons, Cryptobravos did not generate bitcoins through mining at the stated rate—equivalent to about \$325 million per month at then-current prices—and Defendants did not intend to provide a free bitcoin to Customer 1 or allow him to withdraw it. On November 8, 2019, Customer 1 sent one bitcoin to Cryptobravos through Exchange 1. Samson wrote to Customer 1, “1 BTC received. Confirmed for Christmas Package, adding 2 BTCs in on your Trading account in few mins.” This statement was false and

misleading because neither Samson nor Cryptobravos actually gave a bitcoin to Customer 1 pursuant to the Christmas promotion.

39. On December 2, 2019, Samson (using the stage name “Steven Grant”) wrote to Customer 1 that he would “be trading on your account this week with a new Analysis received from the Arbitrage Department so you will see good results in your account soon.” The reference to the Arbitrage Department referred to the concept of arbitrage trading, a trading strategy that seeks to take advantage of price differentials between different virtual currency exchanges—for example, buying bitcoin at a lower price prevailing at one exchange and then selling at a higher price prevailing at another exchange. Samson’s representation was false and misleading because Cryptobravos had no “Arbitrage Department,” and neither Samson nor anyone else in Cryptobravos conducted (or intended to conduct) any arbitrage trading for Customer 1.

40. On December 5, 2019, Samson emailed Customer 1 and several other customers about a “ONCE IN A LIFETIME OPPORTUNITY” to purchase Bitcoin at a steeply discounted price. Samson represented that bitcoin had experienced a “flash crash” on a specific cryptocurrency exchange, losing 90% of its value from approximately \$7,000 to under \$700 before recovering. Samson represented that Cryptobravos had bought a total of 560,000 bitcoin at the lowest flash crash price, and that it would sell them to its customers at discounted prices ranging from 5 bitcoin at \$2,000 each to 10,000 bitcoin at \$750 each. This email was false and misleading because Cryptobravos had not purchased bitcoin during the flash crash and did not intend to sell bitcoin to its customers at the discounted prices; rather, Defendants intended to misappropriate all funds received from Cryptobravos customers.

41. On December 19, 2019, Samson sent a contract for the purchase of bitcoin to Customer 1 in connection with the flash crash deal. Pursuant to the contract, the customer agreed to purchase 100 bitcoin at a price of \$1,000 per bitcoin, with “zero risk involvement.” This contract was false and misleading because it failed to disclose, among other things, that Cryptobravos did not intend to sell bitcoin to Customer 1 and instead intended to misappropriate any funds received. On January 18, 2023, while in the United States, Customer 1 agreed to purchase bitcoin pursuant to the flash crash deal and sent \$25,000 in bitcoin to Cryptobravos through Exchange 1.

42. Defendants ultimately refused Customer 1’s requests for withdrawals and misappropriated his funds. Customer 1’s complete deposit history appears on a spreadsheet maintained by Prokopenko titled “Kharkiv [sic] Wires report.”

43. **Customer 2.** On April 3, 2019, Samson (using the stage name “Daniel Grant”) emailed Customer 2, a United States customer, a document describing a supposed “mining account.” The document solicited deposits between \$25,000 and \$250,000, which would entitle customers to receive a weekly and monthly quota of mined BTC. The document represented that the mined bitcoin would then be traded for profit, including through arbitrage trading. Customer 2 agreed to deposit \$25,000 in a mining account.

44. On April 11, 2019, Samson instructed Customer 2 to open an account with Exchange 1, describing it as “a regulated wallet we work with” that is “located in New York.” This statement was false and misleading because Cryptobravos had no business relationship with Exchange 1. Then, Samson instructed Customer 2 to wire \$25,000 to Exchange 1, convert the funds to bitcoin, and send them to a wallet controlled by Cryptobravos. Customer 2 completed

this transfer on April 17. On April 17, 2019, Samson wrote to Patreanu regarding Customer 2, “25k in.” Patreanu responded, “Good job.”

45. On June 21, 2019, Samson wrote to Customer 2 that he had built a strategy “showing a return of at least 1 Million by Jan 2020, which will open you [sic] an opportunity to buy another House.” On June 24, Samson sent Customer 2 a presentation describing a “Platinum Pension Account.” The presentation stated that Cryptobravos customers experienced a 21,710% return over a five-year period, with an average monthly return of 33.9%. These representations were false and misleading because Cryptobravos misappropriated virtually all of its customers’ money, and therefore its customers did not experience the stated returns. As described further below, Defendants ultimately misappropriated substantially all of Customer 2’s deposits.

46. **Customer 3.** On November 1, 2018, Samson (using the stage name “Daniel Grant”) emailed Customer 3, a United States customer, a spreadsheet purporting to describe a “new trading strategy,” “so you can see exactly how much your Portfolio will generate and what amounts you will receive every month.” Pursuant to the strategy, Customer 3 would deposit \$10,000, and Cryptobravos would execute 100 trades in bitcoin and other virtual currencies on the customer’s behalf over the course of a year, with monthly profits of \$1,200 and a monthly permitted withdrawal of 5% of the account balance. The strategy had a “risk level” of 10%. On November 8, Samson confirmed to Customer 3 that “the funds [for withdrawals] are sent on the monthly basis.” This solicitation was false and misleading because, among other reasons, Cryptobravos conducted little if any trading on its customers’ behalf, and Defendants intended to refuse all requests for withdrawals and misappropriate customers’ funds.

47. On or around November 21, 2018, Customer 3 sent a \$7,000 wire to Cryptobravos from a United States bank. On November 26, 2018, Samson wrote to Customer 3, “I just wanted

to confirm that I have started the trading on your account. . . .” This representation was false and misleading because Samson had not conducted any trades for Customer 3’s account. On December 4, 2018, Samson sent to Patreanu a report on his customers’ deposits for the month of November, which included a \$7,000 deposit from Customer 3.

48. On or around December 27, 2018, Customer 3 wired an additional \$25,000 to Cryptobravos from a United States bank. On January 7, 2019, Samson sent to Patreanu a report on his customers’ deposits for the month of December, which included the \$25,000 deposit from Customer 3.

49. On January 31, 2019, Samson and Customer 3 discussed an additional \$20,000 deposit. Samson wrote to Customer 3, “This Transfer of funds will upgrade your account for Full Arbitration [sic – arbitrage] trades for making about 60% a month profits.” On February 21, 2019, Samson sent Customer 3 an update on his account balance: “The \$7000 in your trading balance have grown now to \$16000. . . . With an additional \$20,000 on this Uptrend Market your account will be easily over \$50,000 within 3 months, and yes you can withdraw next month \$5000 as you need for you[r] [credit] card.” These representations were false and misleading because Samson had conducted no trades and earned no profits on Customer 3’s behalf, and Defendants did not intend to allow a \$5,000 withdrawal.

50. On or around March 22, 2019, Customer 3 wired \$15,000 to Cryptobravos from a United States bank. Samson notified Prokopenko and Patreanu of the wire on the same day. When the wire failed, Samson instructed Customer 3 to transfer the funds to Cryptobravos as bitcoin using Exchange 2, a virtual currency exchange located in New York. Customer 3 completed his deposit by sending bitcoin to Cryptobravos through Exchange 2 on or around

April 15, 2023. The same day, Samson notified Patreanu of the transfer and the identity of the wallet to which the funds were deposited.

51. On or around August 9, 2019, Customer 3 sent another \$30,000 wire transfer from a United States bank to Cryptobravos. Samson informed Patreanu and Prokopenko of the transfer on the same day. On or around August 19, 2019, Customer 3 sent another \$16,000 wire transfer to Cryptobravos. Samson informed Patreanu and Prokopenko of the transfer on the same day. As described below, Cryptobravos ultimately refused Customer 3's requests for withdrawals, and Defendants misappropriated his deposits.

52. **Customer 4.** Defendants also solicited deposits relating to digital assets other than bitcoin. For example, Defendants solicited numerous customers with false promises relating to Libra, a planned virtual currency to be launched by Facebook. In an email to Customer 4 on June 21, 2019, Samson (using the stage name "Daniel Grant") attached a presentation created by Cryptobravos relating to the Libra Coin. The presentation described Libra as a "stablecoin," pegged to existing assets like the dollar or euro." The presentation further described the project as creating a "global currency" that would "allow users to send money to and from each other." In addition, the presentation stated that "the [Libra] coin is likely to reach to peak Bitcoin levels, but the volatility will be about the same as traditional assets like Gold." The presentation then offered customers the opportunity to buy Libra at \$0.5 and sell it for \$1.00:

How can you get Libra? As the minimum requirement to secure coins is only on corporate levels, here at CryptoNXT we have secure [sic] a total investment of \$100m (10 lots of \$10m). Currently, we are reserving private-investor size lots ranging from a minimum of 100,000 to a maximum of 1,000,000 coins per client. Each coin is currently sold for 0.5\$ [sic] and is set to launch at \$1 early 2020.

53. These statements were false and misleading because, among other reasons, Cryptobravos did not have the ability to purchase Libra as described. The presentation also failed to disclose, among other things, that Cryptobravos did not intend to buy Libra on the customer's behalf, and instead, Defendants intended to refuse all requests for withdrawals and misappropriate any funds received. On or around July 25, 2019, Customer 4 sent a \$14,000 wire from a United States bank to Cryptobravos on July 29, 2019. The same day, Samson informed Patreanu and Prokopenko that Customer 4 had made a \$14,000 deposit. Customer 4 sent an additional \$20,000 to Cryptobravos through Exchange 2 on or around November 29, 2019.

54. Ultimately, as described further below, Cryptobravos refused Customer's requests for withdrawals, and Defendants misappropriated his deposits.

C. Defendants' False and Misleading Claims Regarding Withdrawals

55. Although Defendants represented to customers that they could "withdraw money any time," in fact, Defendants almost never allowed customers to withdraw their funds. Instead, when customers requested withdrawals, Defendants offered a range of explanations as to why those withdrawals could not be made. Typically, Defendants instructed customers that their funds could not be returned until the customers paid additional funds, for example, in the form of taxes or commissions. These explanations and instructions were false, as no commissions or taxes were owed. And moreover, even if customers paid additional funds for commissions or taxes, as instructed, Defendants still did not return customers' deposits.

56. On certain occasions, Cryptobravos did allow customers to make small withdrawals. These withdrawals were typically a small percentage of customers' total deposits, and Defendants allowed the withdrawals solely as a way to build a false sense of trust and confidence. Defendants hoped that if they permitted customers to make small withdrawals,

customers could be convinced that their funds were safe and accessible and could then be persuaded to make larger and larger deposits, which the Defendants would then refuse to return.

57. Two specific examples are set forth below, but this pattern was repeated over and over with all of Cryptobravos's customers. Virtually no one who deposited funds with Cryptobravos got their money back.

58. **Customer 2**. On May 16, 2019, Samson wrote to Customer 2 that she could withdraw her funds "immediately" in the case of an emergency. Samson permitted Customer 2 to make small periodic withdrawals from her "mining account" in April, May, June, and July 2019. On September 5, 2019, however, as Customer 2 was attempting to withdraw the balance of her account, Samson told her, "you will need to pay the commissions and then you will receive all your funds." On September 9, 2019, Samson again represented that "once you pay the commission, you are getting all your funds." On September 10, Samson provided the following calculation to Customer 2:

Your Total Earned Funds are \$147,019.98

So the Commission Calculations are below.

Broker Commission: 5% = \$7350.99

Arbitrage Department Trades Commission: 5% = \$7350.99

Tax by the Chinese Government: 25% = \$36,754.99

So the Total Amount you owe us will $\$7350.99 + \$7350.99 + \$36,754.99 = \$51,456.9$

59. These statements were false and misleading. Cryptobravos had conducted no trading on Customer 2's behalf, and therefore Customer 2 had not earned any funds and owed no taxes, and Samson had not earned any commission. Furthermore, Cryptobravos had no ties to the Chinese government.

60. On or around December 4, 2019, Customer 2 told Samson that she was attempting to take out a high interest loan for \$10,000 to cover a portion of the supposed taxes and commissions. The next day, Samson responded that he would send funds from her account “no later than 1 hour from the receipt of your transfer.” On January 6, 2020, Customer 2 wrote to confirm, “I’m just checking in to make sure I can give you money to get my funds back?” Samson responded, “Yes, you can pay the funds and withdraw your complete account.” When Customer 2 was unable to come up with \$10,000, Samson wrote to Customer 2 on March 4, 2020, “I understand you have \$5,000 available now, please arrange more \$5,000 and clear this as you will receive your Portfolio worth almost \$200,000 within 24-48 Hours in your hands.” In late March, 2020, Customer 2 received a high interest loan for \$2,000. Following Samson’s instructions, on or around March 27, 2020, Customer 2 wired the money to Exchange 1, converted it to bitcoin, and sent it to a wallet controlled by Defendants. The same day, Samson responded, “they put your withdrawal on Hong Kong Exchange already. Currently status in line pending but should go through. Without [sic] 48 hours I think you should have them in your wallet.” Samson attached an image purporting to show a transfer of over 34 bitcoin to Customer 2. However, Customer 2 never received a withdrawal.

61. **Customer 4.** On October 24, 2019, Samson represented to Customer 4 that if Customer 4 deposited an additional \$15,000, he would be able to withdraw it again during the Christmas holiday. Customer 4 responded that he would like to retire in January and draw \$9,000 per month from his account with Cryptobravos to fund his retirement. Samson responded, “yes that can be done no problem.” On October 31, 2019, Customer 4 deposited an additional \$11,000 with Cryptobravos. On November 1, 2019, Prokopenko sent a report to Hananya showing this transfer. On November 5, 2019, Customer 4 wrote to Samson that he was

working on a \$20,000 loan for an additional deposit. The same day, Samson wrote to “Adam Anderson,” “you think we should send him 4k to get this 20k? as you know he did it 2 times what he said, he will get the money if we send him 4k.” On November 7, 2019 Samson sought approval from Anderson to allow the withdrawal, writing, “I already received from him 11k last month and he is sending another 20k this month.” The same day, Samson notified Customer 4 that the \$4,000 withdrawal had been approved. The allowance of this withdrawal was misleading because it was intended to provide false assurance to Customer 4 that future withdrawals would also be permitted and was intended to induce future deposits that Defendants intended to misappropriate. Thereafter in November 2019, Samson worked to convince Customer 4 to take out private and personal loans, including from his son and cousin, totaling \$20,000.

62. On November 21, 2019, Samson sent Customer 4 a buy-one-get-one-free contract for the purchase of bitcoin, pursuant to which Customer 4 would receive six bitcoin for his \$20,000 deposit. On November 27, 2019, Customer 4 told Samson that a friend was willing to wire him \$20,000 for an additional deposit. Customer 4 wired these funds to Cryptobravos on November 29, 2019. The same day, Samson sent the wire confirmation to Prokopenko. On December 2, 2019, Customer 4 wrote to Samson asking to ensure that the six bitcoins were deposited in Customer 4’s account at Exchange 2 immediately, so that Customer 4 could pay back his friend for the loan. Samson responded that he would shortly send a confirmation for the transfer of six bitcoin as well as a withdraw of \$5,500. Later in the day, Samson wrote to Customer 4, “the funds are sent I think you should see them by the evening.” On December 4, 2019, Samson wrote to another employee of Cryptobravos using the stage name “Sunny Augustine”:

Greetings! Please note and notify support that the following clients from NXT will bug you guys by phone calls and emails for not receiving their withdrawals in their wallets as I sent them a confirmation (Not real). . . . [Customer 4] So you know already what to do here as we will not be calling them at the moment. But, I will reassign them for account closures in a week with a new agent.

63. Customer 4 received no further withdrawals from Cryptobravos.

D. Defendants' Knowledge of Fraud and Deceit

64. Each of the Defendants knew or recklessly disregarded that Cryptobravos had no legitimate purpose and was simply a vehicle for fraud. Each of the Defendants knew or recklessly disregarded that Cryptobravos employees made numerous false and misleading statements to customers and then refused to allow withdrawals.

65. Samson spoke directly with customers and knew or recklessly disregarded that the statements he was making were false and misleading. As an account manager, Samson communicated regularly with his customers, had primary responsibility for overseeing their accounts, and was compensated based on the volume of his customers' deposits. In this capacity, Samson knew the full details of each of his customers' deposits, withdrawals, commissions, and transactions. Samson therefore knew or recklessly disregarded that Cryptobravos executed no actual transactions on its customers' behalf and that every statement he made to customers about those transactions was false or misleading. Samson also knew or recklessly disregarded that none of his customers received meaningful withdrawals, and he therefore knew or recklessly disregarded that every statement he made to customers about their ability to withdraw funds was false and misleading.

66. Although Patreanu, Hananya, and Prokopenko typically did not communicate directly with customers, they collectively directed and controlled all aspects of Cryptobravos, including its finances and banking relationships. In light of their complete control of

Cryptobravos and the pervasive nature of the fraud, which encompassed substantially all of Cryptobravos's customers, the Controlling Defendants knew—or at best, recklessly disregarded—that employees of Cryptobravos were as a course of business lying to customers and refusing virtually all requests for withdrawals. Patreanu, Hananya, and Prokopenko received and maintained regular reports regarding customer deposits and withdrawals, which demonstrated that while Cryptobravos took in tens of millions of dollars in deposits, it disbursed only a small fraction of that amount in withdrawals.

67. The Controlling Defendants were also aware of specific customer complaints regarding Cryptobravos's refusal to permit withdrawals. For example, on November 15, 2018, Samson wrote to Patreanu and other employees with the stage names "William Mayers," "Ross Malone," and "Sunny Augustine" regarding a "legal issue threat" from a customer who indicated she would hire a lawyer to get her money back from Cryptobravos. "Mayers" responded, copying Patreanu: "Ross[,] Daniel [Grant, i.e., Samson] can we take more form [sic] her." Samson responded, copying Patreanu, "The way she talked to me i dont [sic] see a point." "Malone" responded, copying Samson and Patreanu, "bro shes [sic] a freaking layer [liar] lol." Samson responded, copying Patreanu, "ok I will try again then."

68. On December 10, 2018, Prokopenko received an email from Customer 5, who had deposited over \$50,000 in Cryptonxt that he was unable to withdraw. Customer 5 wrote, "I await a complete explanation as to where all my hard earned money is and how this bad situation can be rectified." Prokopenko forwarded this email to Patreanu and Hananya.

69. On December 12, 2018, an independent third party payment services provider used by Cryptobravos to receive customer funds sent a "Notice of Suspected Fraudulent Transactions" to Prokopenko regarding Customer 6. The payment services provider wrote: "We

write to inform you that we received a complaint in relation to your services granted to [Customer 6]. We are aware, from correspondence with [Customer 6's] lawyer, that you have been informed about this case already." Prokopenko forwarded this email to Patreanu and Hananya. In further correspondence, on January 11, 2019, the payment services provider wrote to Prokopenko, "There is absolutely no evidence, that we are aware of, which suggests that you provided [Customer 6] with the services or products which were offered or sold to him." Prokopenko forwarded this email to Patreanu and Hananya. On January 14, 2019, Prokopenko wrote to the payment services provider that Customer 6 "Lost money in trading." This was false and misleading because, as Defendants all knew, Cryptobravos conducted little or no trading on behalf of Customer 6. Prokopenko forwarded this email to Patreanu and Hananya.

70. The Controlling Defendants also knew that Cryptobravos employees were charging taxes for non-existent profits and then closing accounts and misappropriating the funds when customers either could not or would not pay the supposed taxes. For example, on May 13, 2019, Samson sent the following email to Customer 7, who had deposited over \$500,000 with Cryptobravos: "I will like to inform you sadly that unfortunately we will not be able to proceed with your account, due to lack of communication and the non payment of the funds for the taxation." And on May 28, 2019, Samson wrote to Customer 7, "In case you will not send today the remaining 130K, you will have to send all the TAX payment which is 750K." Samson forwarded these emails to Patreanu.

71. On October 30, 2019, a Cryptobravos employee emailed Patreanu and Hananya, addressing them collectively as "Management," attaching a notification from the United States Consumer Financial Protection Bureau, notifying Cryptobravos (specifically, the Tradenix brand) that the CFPB had received one or more complaints regarding the company.

72. The Controlling Defendants were also aware of the substance of Cryptobravos's calls with its customers. Patreanu, for example, circulated at least two proposed call scripts to others within the organization. Patreanu and Hananya also reviewed other scripts for use by Cryptobravos in its solicitation of customers. For example, on December 2, 2019, a Cryptobravos employee emailed Patreanu and Hananya, addressing them collectively as "Management":

Below you can see our speeches for e-wallet dept, screenshots that we opened with clients and call recordings to my agents.

Please let us know if we need to add or remove anything.

PS: We made a trial w[ith] [Crypto]NXT we are waiting your strategic changes for other platforms

73. Below this, the call center employee copied three different scripts for the purpose of inducing customers to set up digital wallets to receive a supposed "bonus" offered by Cryptobravos.

74. The Controlling Defendants were even aware of the substance of specific telephone conversations between Cryptobravos employees and customers. Such calls were frequently recorded, and Patreanu and Hananya received emails attaching specific calls of interest. For example, on October 3, 2019, a Cryptobravos "QC Department Manager" sent Patreanu and Hananya a recording in which a Cryptobravos employee offered to contact a customer using the employee's personal WhatsApp account. In the recording, the Cryptobravos employee can be heard pressuring a customer to go to the bank for the purpose of sending funds to Cryptobravos. When the customer says, "that's all the money I have," the call center employee responds, "that's why . . . we agreed that when we make this deal, you start withdrawing money back to yourself." This representation was false and misleading because

Cryptobravos refused virtually all requests for withdrawals—a fact that the Controlling Defendants well knew.

75. On November 22, 2019, the QC Department Manager sent another call recording to Patreanu and Hananya. During the recorded call, the call center employee made numerous misrepresentations, including that:

- Cryptobravos’s headquarters was in New York, citing as evidence the fact that he had called the customer using a New York telephone number;
- Cryptobravos “works with New York regulations”;
- Cryptobravos maintained offices in London and Switzerland;
- The Cryptobravos employee was a licensed broker who had worked for several prominent Wall Street firms;
- Cryptobravos takes commissions based on the customers’ profits, and not based on the amount of the customer’s deposits;
- The customer would be able to withdraw funds from his account.

76. These representations were false and misleading because, as the Controlling Defendants knew, Cryptobravos had no offices in New York, London, or Switzerland; Cryptobravos was not registered with any New York regulatory agency; the call center employee was not a licensed broker; Cryptobravos call center employees earned commissions on deposits, not trading profits; and, Cryptobravos did not conduct trades on behalf of clients, but rather, misappropriated virtually all money deposited. In his email to Patreanu and Hananya attaching the recording, the QC Department Manager emphasized the fact that the call center employee represented to the customer that Cryptobravos was “regulated in New York.”

77. On November 22, 2019, the QC Department Manager sent another call recording to Patreanu and Hananya. During the recorded call, the call center employee made numerous misrepresentations, including that:

- The customer's \$200,000 deposit had grown to \$1 million;
- Cryptobravos takes commissions based on the customers' profits, and not from the amount the customer's deposits;
- There was no risk that the customer would lose all of the money in her account;
- The customer would be able to withdraw funds from her account at any time;
- If the customer wished to withdraw money from her account now, she would owe 25% of the account balance in taxes that must be paid to Cryptobravos before a withdrawal could be made, and that Cryptobravos would send the tax payment "to the government";
- If the customer requested a withdrawal and paid 25% of the balance in taxes, Cryptobravos would send her the amount of the withdrawal "right away";
- Cryptobravos was not a scam company.

78. These representations were false and misleading because, as the Controlling Defendants knew, Cryptobravos had not executed any transactions on the customer's behalf, and her account balance had not grown; Cryptobravos call center employees earned commissions on deposits, not trading profits; the customer did not owe any taxes; and Cryptobravos was a scam company that misappropriated virtually all money deposited, including money paid towards so-called "taxes."

79. On March 26, 2019, the VP of Sales of the Albanian call center sent three other call recordings to Patreanu and Hananya. During the recorded calls, the call center employees made numerous misrepresentations, including that:

- Cryptobravos made profits for customers by trading cryptocurrency;
- The customer would not lose money on their account, and Cryptobravos could guarantee a profit;
- The broker was supported by analysts who advised on transactions to ensure profitability.

80. These statements were false and misleading because, as the Controlling Defendants knew, Cryptobravos did not place trades on its customers' behalf and had no analysts to advise on these non-existent trades.

E. Patreanu's and Hananya's Control Over Customer Funds

81. Patreanu's and Hananya's knowledge of fraud and control over Cryptobravos is also evidenced by their control over virtual currency wallets associated with Cryptobravos.

82. Because Cryptobravos misappropriated tens of millions of dollars in bitcoin from its customers, Patreanu and Hananya needed a way to exchange large volumes of virtual currency for fiat currency. To accomplish this, Patreanu and Hananya engaged the services of Individual 1, a Florida resident. Between 2019 and 2021, Individual 1, generally acting through Company 1, a Florida limited liability company, bought at least \$8 million in bitcoin (at then-current prices) from Patreanu and Hananya. Individual 1 and Company 1 frequently paid for this bitcoin through wire transfers from banks in the United States. Patreanu and Hananya directed Individual 1 to wire money to companies around the world, including over \$3 million to Expected Value Plus and over \$600,000 to NEK Marketing.

83. The wallets from which Patreanu and Hananya sent bitcoin to Individual 1 were associated with Cryptobravos. For example, on February 6, 2019, Individual 2, an associate of Patreanu who facilitated Patreanu's sale of bitcoin to Individual 1, instructed Individual 1 to send bitcoin to Wallet Address 1 for receipt by Patreanu. The same wallet address appears in a document maintained by Cryptobravos listing wallet addresses used by Cryptobravos in connection with the fraud.

84. Patreanu's and Hananya's control over these wallets further demonstrates their knowledge of fraud. Patreanu and Hananya knew that they were selling the bitcoin received

from Cryptobravos's customers rather than depositing it in customers' accounts and therefore knew that Cryptobravos was conducting little or no trading on its customers' behalf and was simply misappropriating the funds it received from its customers.

F. Defendants' Concealment of the Fraudulent Scheme

85. Throughout the Relevant Period, Patreanu and Hananya misrepresented the nature of their business to the banks they used to facilitate their fraudulent scheme.

86. For example, on March 25, 2020, after receiving notice that Bank 2 intended to close Expected Value Plus's account, Patreanu wrote to Bank 2 "to give you some background regarding [Expected Value Plus] so you will understand better the company core business as well as its incomes." Patreanu wrote that Expected Value Plus "is a Consulting services company specializing in marketing quality control as well as management Workers training for client [sic] in the sales business" and that Expected Value Plus also "offer[s] professional training for clients in management consultation" as well as "data management business development services." He represented that Company 1 was "one client [to which Expected Value Plus] is giving the above services" and that Company 1 had made payments to Expected Value Plus for these services pursuant to invoices sent from Expected Value Plus to Company 1. In his correspondence with Bank 2, Patreanu attached a purported contract between Expected Value Plus and Company 1 for consulting and marketing services, as well as purported invoices reflecting amounts to be paid by Company 1 to Expected Value Plus pursuant to the contract and for "online marketing strategy," "data cleaning," and "marketing analysis."

87. This communication was false and misleading. Expected Value Plus was not a "consulting services company," but rather, a front company used by Patreanu and Hananya to perpetrate their fraudulent scheme. Payments made by Company 1 to Expected Value Plus were

for the purpose of buying bitcoin from Cryptobravos that had been misappropriated from Cryptobravos customers, not for the payment of services performed by Expected Value Plus—and indeed, Expected Value Plus sent no invoices to (and performed no services for) Company 1 at any time. The invoices were fake, created by Hananya for the purpose of deceiving Bank 2. The purported contract between Expected Value Plus and Company 1 was also fake and created for the purpose of deceiving Bank 2. In reality, no such contract ever existed between those companies.

V. VIOLATIONS OF THE COMMODITY EXCHANGE ACT AND REGULATIONS

Count I—Fraud by Deceptive Device or Contrivance

Violations of Section 6(c)(1) of the Act, 7 U.S.C. § 9(1), and Regulation 180.1(a)(1)-(3), 17 C.F.R. § 180.1(a)(1)-(3) (2022)

88. Paragraphs 1 through 87 are re-alleged and incorporated herein by reference.

89. 7 U.S.C. § 9(1), makes it unlawful for any person, directly or indirectly, to:

[U]se or employ, or attempt to use or employ, in connection with any swap, or a contract of sale of any commodity in interstate commerce, or for future delivery on or subject to the rules of any registered entity, any manipulative or deceptive device or contrivance, in contravention of such rules and regulations as the Commission shall promulgate by not later than 1 year after [July 21, 2010, the date of enactment of the Dodd-Frank Wall Street Reform and Consumer Protection Act]

90. 17 C.F.R. § 180.1(a), provides in part:

It shall be unlawful for any person, directly or indirectly, in connection with any swap, or contract of sale of any commodity in interstate commerce, or contract for future delivery on or subject to the rules of any registered entity, to intentionally or recklessly:

(1) Use or employ, or attempt to use or employ, any manipulative device, scheme, or artifice to defraud;

(2) Make, or attempt to make, any untrue or misleading statement of a material fact or to omit to state a material fact necessary in order to make the statements made not untrue or misleading;

(3) Engage, or attempt to engage, in any act, practice, or course of business, which operates or would operate as a fraud or deceit upon any person

91. During the Relevant Period, as described above, Defendants violated 7 U.S.C. § 9(1) and 17 C.F.R. § 180.1(a)(1)-(3) by, among other things, in connection with contracts of sale of commodities in interstate commerce, or for future delivery, making untrue or misleading statements of material fact or omitting to state material facts necessary in order to make statements made not untrue or misleading, including but not limited to the following:

- A. Misrepresenting that customers' deposits would be "risk-free";
- B. Misrepresenting that customers would be able to make withdrawals from their accounts at any time;
- C. Issuing performance statements and updates misrepresenting the supposed amount of bitcoins and profits in each customer's purported account(s);
- D. Misrepresenting the profitability of Defendants' virtual currency trading to prospective and existing customers;
- E. Failing to disclose, and omitting, that Defendants never achieved the advertised performance and returns for customers;
- F. Failing to disclose, and omitting, that Defendants were not executing transactions as promised but rather were misappropriating customer deposits;
- G. Misrepresenting that customers owed commissions or taxes before withdrawals could be made from their accounts.

92. During the Relevant Period, as described above, Defendants violated 7 U.S.C. § 9(1) and 17 C.F.R. § 180.1(a)(1)-(3) by using or employing, or attempting to use or employ, a manipulative device, scheme, or artifice to defraud.

93. During the Relevant Period, as described above, Defendants violated 7 U.S.C. § 9(1) and 17 C.F.R. § 180.1(a)(1)-(3) by engaging, or attempting to engage, in acts,

practices, or courses of business, which operate or would operate as a fraud or deceit upon any person.

94. Defendants engaged in the acts and practices described above willfully, intentionally, or recklessly.

95. Each act of: (1) using or employing a manipulative device, scheme, or artifice to defraud; (2) making untrue or misleading statements of material fact, or omitting to state material facts necessary to make the statements not untrue or misleading; and (3) engaging in any act, practice, or course of business, which operated or would operate as a fraud or deceit upon any person, including but not limited to those specifically alleged herein, is alleged as a separate and distinct violation of 7 U.S.C. § 9(1) and 17 C.F.R. § 180.1(a)(1)-(3).

96. Patreanu, Hananya, and Prokopenko held and exercised direct and indirect control over Cryptobravos and either did not act in good faith or knowingly induced violations of 7 U.S.C. § 9(1) and 17 C.F.R. § 180.1(a)(1)-(3) by Cryptobravos and its employees. As a controlling person of Cryptobravos, Patreanu, Hananya, and Prokopenko are liable for violations of 7 U.S.C. § 9(1) and 17 C.F.R. § 180.1(a)(1)-(3) by Cryptobravos and its employees pursuant to Section 13(b) of the Act, 7 U.S.C. § 13c(b).

97. Patreanu, Hananya, and Prokopenko willfully aided, abetted, counseled, commanded, induced, or procured the commission of the acts constituting violations of 7 U.S.C. § 9(1) and 17 C.F.R. § 180.1(a)(1)-(3), committed by Samson and other Cryptobravos agents and employees. Pursuant to Section 13(a) of the Act, 7 U.S.C. § 13c(a), Patreanu, Hananya, and Prokopenko are therefore responsible as if they were a principal for Samson's and Cryptobravos employees' violations of 7 U.S.C. § 9(1) and 17 C.F.R. § 180.1(a)(1)-(3).

VI. RELIEF REQUESTED

WHEREFORE, the Commission respectfully requests that the Court, as authorized by Section 6c of the Act, 7 U.S.C. § 13a-1, and pursuant to its own equitable powers, enter:

- A. An order finding that Defendants violated Section 6(c)(1) of the Act, 7 U.S.C. § 9(1), and Regulation 180.1(a)(1)-(3), 17 C.F.R. § 180.1(a)(1)-(3) (2022);
- B. An order of permanent injunction enjoining each Defendant and any other person or entity associated with them, including but not limited to affiliates, agents, servants, employees, assigns, attorneys, and all persons in active concert or participation with Defendants, including any successor thereof, from:
 - i. Engaging, directly or indirectly, in conduct in violation of 7 U.S.C. § 9(1) and 17 C.F.R. § 180.1(a)(1)-(3);
 - ii. Trading on or subject to the rules of any registered entity (as that term is defined in Section 1a(40) of the Act, 7 U.S.C. § 1a(40));
 - iii. Entering into any transactions involving “commodity interests” (as that term is defined in Regulation 1.3, 17 C.F.R. § 1.3 (2022)), or digital asset commodities, for their own personal account(s) or for any account in which Defendants have a direct or indirect interest;
 - iv. Having any commodity interests or digital asset commodities traded on Defendants’ behalf;
 - v. Controlling or directing the trading for or on behalf of any other person or entity, whether by power of attorney or otherwise, in any account involving commodity interests or digital asset commodities;

- vi. Soliciting, receiving, or accepting any funds from any person for the purpose of purchasing or selling commodity interests or digital asset commodities;
 - vii. Applying for registration or claiming exemption from registration with the Commission in any capacity, and engaging in any activity requiring such registration or exemption from registration with the Commission, except as provided for in Regulation 4.14(a)(9), 17 C.F.R. § 4.14(a)(9) (2022); and/or
 - viii. Acting as a principal (as that term is defined in Regulation 3.1(a), 17 C.F.R. § 3.1(a) (2022)), agent, or any other officer or employee of any person (as that term is defined in Section 1a(38) of the Act, 7 U.S.C. § 1a(38)), registered, exempted from registration, or required to be registered with the Commission except as provided for in 17 C.F.R. § 4.14(a)(9);
- C. An order requiring Defendants to pay civil monetary penalties of not more than the civil monetary penalty prescribed by Section 6c(d)(1) of the Act, 7 U.S.C. § 13a-1(d)(1), as adjusted for inflation pursuant to the Federal Civil Penalties Inflation Adjustment Act Improvements Act of 2015, Pub. L. 114–74, 129 Stat. 584, title VII, Section 701, *see* Commission Regulation 143.8, 17 C.F.R. § 143.8 (2022), for each violation of the Act or Regulations, plus post-judgment interest;
- D. An order directing Defendants, as well as any successors thereof, to disgorge, pursuant to such procedure as the Court may order, all benefits received

including, but not limited to, trading profits, revenues, salaries, commissions, fees, or loans derived directly or indirectly from acts or practices which constitute violations of the Act and Regulations, as described herein, and pre- and post-judgment interest thereon from the date of such violations;

- E. An order directing Defendants, as well as any successors thereof, to make full restitution, pursuant to such procedure as the Court may order, to every customer whose funds Defendants received, or caused another person or entity to receive, as a result of the acts and practices constituting violations of the Act and Regulations, as described herein, and pre- and post-judgment interest thereon from the date of such violations;
- F. An order directing Defendants, as well as any successors thereof, to rescind, pursuant to such procedure as the Court may order, all contracts and agreements, whether express or implied, entered into between, with, or among Defendants and any customer whose funds were received by Defendants as a result of the acts and practices which constituted violations of the Act and the Regulations, as described herein;
- G. An order directing that Defendants, and any successors thereof, make an accounting to the Court of all of their assets and liabilities, together with all funds they received from and paid to customers and other persons in connection with commodity transactions and all disbursements for any purpose whatsoever of funds received from commodity transactions, including salaries, commissions, interest, fees, loans, and other disbursement of money or property of any kind from at least the beginning of the Relevant Period to the date of such accounting;

- H. An order requiring Defendants and any successors thereof to pay costs and fees as permitted by 28 U.S.C. §§ 1920 and 2412(a)(2); and
- I. An order providing such other and further relief as the Court deems proper.

* * *

VII. DEMAND FOR JURY TRIAL

Plaintiff hereby demands a jury trial.

Dated: September 29, 2023

**COMMODITY FUTURES TRADING
COMMISSION**

By: /s/ John C. Murphy
John C. Murphy
Trial Attorney
jmurphy@cftc.gov
Phone: (646) 746-9700

K. Brent Tomer
Chief Trial Attorney
ktomer@cftc.gov
Phone: (646) 746-9700

Manal M. Sultan
Deputy Director
msultan@cftc.gov
Phone: (646) 746-9700

Commodity Futures Trading Commission
Division of Enforcement
290 Broadway, 6th Floor
New York, NY 10007
Phone: (646) 746-9700
Fax: (646) 746-9940

ATTORNEYS FOR PLAINTIFF
COMMODITY FUTURES TRADING
COMMISSION