

United States District Court
District of New Jersey

UNITED STATES OF AMERICA

v.

CHRISTOPHER CASTELLUZZO

:
:
:
:
:
:
:
:

FILED UNDER SEAL

Mag. No. 25-16093 (JRA)

CRIMINAL COMPLAINT

I, the undersigned complainant, being duly sworn, state the following is true and correct to the best of my knowledge and belief.

SEE ATTACHMENT A

I further state that this Complaint is based on the following facts:

SEE ATTACHMENT B

continued on the attached pages and made a part hereof.

Andrew Gray

Special Agent Andrew Gray
Federal Bureau of Investigation

Special Agent Gray attested to this Complaint
by telephone pursuant to F.R.C.P. 4.1

June 27, 2025 at
Date

District of New Jersey
County and State

Honorable José R. Almonte
United States Magistrate Judge

Jose R. Almonte
Signature of Judicial Officer

ATTACHMENT A

(Conspiracy to Commit Money Laundering)

From in or around 2015 through in or around July 2022, in Union, Hudson and Essex Counties, in the District of New Jersey, and elsewhere, the defendant,

CHRISTOPHER CASTELLUZZO,

did knowingly and intentionally conspire and agree with other persons, known and unknown, to conduct and attempt to conduct financial transactions in and affecting interstate and foreign commerce, which involved the proceeds of specified unlawful activity—that is, conspiracy to distribute and possess with intent to distribute a controlled substance—knowing that the transaction was designed in whole and in part to conceal and disguise the nature, location, source, ownership, and control of the proceeds of specified unlawful activity, and knowing that the property involved in the financial transactions represented the proceeds of some form of unlawful activity, contrary to Title 18, United States Code, Section 1956(a)(1)(B)(i).

In violation of Title 18, United States Code, Sections 1956(h) and 2.

ATTACHMENT B

I, Andrew Gray, am a Special Agent with the Federal Bureau of Investigation (“FBI”). I am fully familiar with the facts set forth herein based on my own investigation, my conversations with other law enforcement officers, and my review of reports, documents, and items of evidence. Because this complaint is being submitted for the limited purpose of establishing probable cause, I have not set forth each and every fact that I know concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause. Unless specifically indicated, all dates, times, and transaction amounts referenced herein are approximate, and all conversations and statements described are related in substance and in part.

Background of Drug Distribution and Cryptocurrency Proceeds

1. Since in or around 2021, the FBI has been investigating a group of individuals, including the defendant, Christopher Castelluzzo (the “defendant”), who have been engaged in a scheme to launder the proceeds of illegal drug distribution.

2. The defendant and one of his co-conspirators in the money laundering conspiracy (“Conspirator-1”) were indicted in August 2013 in the District of New Jersey for conspiring to and in fact importing methylone, a Schedule I controlled substance, into the United States. Trial on these charges did not begin until nearly two years later. The defendant and Conspirator-1 continued their criminal drug enterprise during the intervening period while they were out on pre-trial release.

3. During this time, the defendant and Conspirator-1 sold narcotics on darknet marketplaces. “Darknet marketplaces” are commercial websites that are typically hosted as Tor onion services. Darknet marketplaces primarily function as black markets where one can sell or broker transactions involving illegal drugs, cybercriminal tools (e.g., malware), weapons, counterfeit currency, stolen personally identifiable information, forged documents and identification credentials, and other illicit goods and services. BTC is the most common method of payment for products and services procured on darknet marketplaces.

4. Conspirator-1 marketed controlled substances on the darknet marketplaces and tracked and managed their cryptocurrency earnings and business expenses. Defendant helped obtain narcotics at wholesale prices.

5. Conspirator-1 began using a Silk Road account in or around the summer of 2013, and the defendant and Conspirator-1 quickly began to profit by purchasing large amounts of methylone from China, creating distributable amounts, and selling the drugs on the darknet marketplace for a substantial

profit. They began to receive positive reviews on Silk Road—which was crucial in the darknet narcotics business—and business grew quickly. During this time, defendant and Conspirator-1 also bought large amounts of cocaine at wholesale prices, breaking down cocaine into smaller amounts, selling the cocaine on darknet marketplaces, and sending it to customers through the mail. Defendant and Conspirator-1 sometimes sent 50 or 60 packages of narcotics per day.

6. New Jersey state law enforcement investigated the defendant and Conspirator-1 for this illegal drug trafficking business and intercepted some of their phone calls, which revealed the pair talking about drug proceeds comprised at least in part of Bitcoin. For example, during an intercepted call on or about February 20, 2015, the defendant and Conspirator-1 discussed their financial records, including the flow of money in and out of their partnership in the form of U.S. currency and Bitcoin. Conspirator-1 told the Defendant, “...he gave me two and I took one thousand in Bitcoins....I took one thousand dollars in Bitcoins, right? That I took off the tab. He paid, he gave me two thousand dollars....” Based on my training and experience, Defendant was explaining that he accepted from a customer, in exchange for the sale of narcotics, two thousand dollars in fiat currency and one thousand dollars worth of Bitcoin.

7. During a lawfully intercepted call on or about March 26, 2015, defendant and Conspirator-1 discussed a plan to build a website around Bitcoin and use a programmer to help them put it on a “.onion”:¹

Defendant: So what would happen is, the site gets fucking popping, they look at that shit they find out who made it. They come to these programmers and designers like its them, and they gonna be like no, I made it for this person, so it would be made from day one you know

Conspirator-1: Masking your identity, like that's the easy part, masking your identity

Defendant: Alright so what I'm saying is that's how it gets done bro, that's how it gets done.

Conspirator-1: Alright well they're gonna build this shit

¹ Within the Tor network itself, entire websites can be set up as “onion services.” “Onion services” operate in the same way as regular public websites with one critical exception: the IP address for the web server is hidden and instead is replaced with a Tor-based web address, which is a series of algorithm-generated characters followed by the suffix “.onion.”

around credit cards

Defendant: No, no you tell you **want it built around bitcoins.**

Conspirator-1: They're gonna know exactly what you're building

Defendant: It doesn't matter if they know what you're building. You're building it on the Clearnet first of all, second of all, you're fucking giving them identification or whatever what are they gonna do. What can they do? My nigga, you're building a bitcoin auction place, that's it.

(emphasis added). Based on my training and experience, and the federal prosecution of the defendant and Conspirator-1 that resulted in drug conspiracy convictions, I have probable cause to believe that defendant and Conspirator-1 were discussing how to build a darknet website selling narcotics where purchasers could use bitcoin to buy drugs instead of credit cards.

8. During another lawfully intercepted call on or about March 26, 2015, the defendant and Conspirator-1 discussed trying to make \$50 million through their darknet mail-order website and how they can use Bitcoin to launder or “wash” the illegal proceeds. They discussed another individual who laundered approximately \$50 million through BTC-e. Using this as an example, they discussed how they could “wash” coins in a similar fashion:

Defendant: Fifty mil

Conspirator-1: Fifty mil bro, in fucking fourteen months.

Defendant: Let me get that

Conspirator-1: Yo hmm, the guy was trying to cash the shit out for BTCE, BTCE fucking uh jerked for like fucking uh like two thousand coins.

Defendant: Are you serious?

Conspirator-1: Yeah

Defendant: How did they know?

Conspirator-1: The people are following the coins, and there was like requests put into BTCE to fucking seize those coins and BTCE just fucking took em, hehe and didn't fucking withdraw em to the addresses, altered the withdrawals on the coins. **Guy was trying to wash them through BTCE, cause you know when you send coins into an exchange and then you do a withdrawal out from the exchange, it comes back from a different coin address**

Defendant: Yeah

Conspirator-1: **That's why its, it's a perfect way to wash coins**

Defendant: Oh my god, the coins are low as hell now

Conspirator-1: Yeah they're like two fifty

Defendant: Yeah this is the first time I looked at this shit in a minute. So two fifty, two fifty times

Conspirator-1: He got away with a hundred and thirty thousand coins

Defendant: Oh, so he didn't even care, they jerked him for like a halfa mil. So BTCE do to it? They kept it themselves or

Conspirator-1: I don't know, he just didn't fucking let him withdraw it. I didn't really follow up on the story.

Defendant: Yo, imagine if we got off with fifty mil and then some shit like that happen to us

Conspirator-1: Well, first of all, the way I'd wash it is I'd start I'd start like minimally like I'd be doing like fifty/hundred coins through like hit mixer dot 10, and once the hit mixer dot 10 doesn't fill one of my withdrawals, I fucking go into the ground, fucking figure

something else out. **Wash a little bit through local bitcoins, fucking like I don't need all the fifty mil like right there and then, I just need it to be washed, it might take me fucking a few months to wash them, definitely gonna take me a few months to wash them.**

Defendant: I don't know

Conspirator-1: But figure what's a hundred and thirty thousand divided by a hundred, a hundred and thirty?

Defendant: Yeah

Conspirator-1: Hundred and thirty days to fucking wash those coins. Which is four months, four and a half months.

(emphases added). Based on my training and experience, I have probable cause to believe that the defendant and Conspirator-1 were discussing the fact that Bitcoin withdrawn from a cryptocurrency exchange come back from a different Bitcoin address from which it was sent, making it an effective way to “wash” or launder the Bitcoin from their illegal drug sales by moving it in and out of cryptocurrency exchanges.

9. On May 29, 2015, after an approximately week-long trial, a federal jury found defendant and Conspirator-1 guilty of conspiracy to distribute and possess with intent to distribute controlled substances. In 2016, defendant was sentenced to 240 months' imprisonment, and Conspirator-1 was sentenced to 220 months' imprisonment. On August 1, 2016, Conspirator-1 pled guilty in New Jersey state court to leading a narcotics trafficking network in violation of N.J.S.A. 2C:35-3 and was sentenced to 19 years' imprisonment and 193 months of parole ineligibility, which was to run concurrently to his federal sentence. On May 24, 2018, defendant also pled guilty to leading a narcotics trafficking network in violation of N.J.S.A. 2C:35-3 and was sentenced to 21 years' imprisonment and 214 months of parole ineligibility, which was to run concurrently to his federal sentence. The defendant remains detained in federal prison serving the completion of his federal sentence.

Conspirator-2 Joins the Conspiracy

10. Defendant and Conspirator-1 also discussed who would be able to help them execute the plan and put a website on .onion. Specifically, they discussed using an individual (“Conspirator-2”)—who, based on the intercepted

calls, appeared to be visiting New Jersey at the time—to help them build a site on .onion. On or about March 27, 2015, law enforcement intercepted a call between Conspirator-1 and Conspirator-2. During the call, Conspirator-1 and Conspirator-2 discussed how Conspirator-2 could help with the defendant's and Conspirator-1's darknet website to sell narcotics:

Conspirator-2: I gotcha. Yea you could put it together look like I said there's a there's there's the most probable way of doing it, which I'm you know which I'm 90% time gonna work if um if if if if we gotta get shadier than that in terms of of taking you off the network, then you know we'll build a tor router out of a razz pi and you put that behind it and that's a project I've been wanting to do anyway so um yea go ahead, run it through, run the whole thing through [U/I] and that oughta be enough to to to mask everything and um [U/I].

Conspirator-1: Router?

Conspirator-2: What?

Conspirator-1: How do you build a tor router?

Conspirator-2: Dude people are taking razz pi's right, people are taking razz pi's and they're putting them in cases and they're creating wireless hot spots that um produce a wireless hot spot, you connect to it, but the router itself connects up to the tor network so anything that connects to that wireless router to the hot spot uh it runs through tor.

Conspirator-1: You can just buy these things?

Conspirator-2: No you uh... somebody tried the kick starter one and sell it, it didn't catch on. People are building them out of uh razz pi's, which is like a 35 dollar computer.

Conspirator-1: Right, do you know how to build one?

Conspirator-2: Uh I could build one for you, yea. Shouldn't even be that difficult, um I'll let you know how much the parts cost and uh there's plans all over the place. I'll build one for ya.

Conspirator-1: Okay [U/I] let me get one of those man. Alright?

Conspirator-2: You got it, you got it, [U/I] tonight man.

Conspirator-1: I'm gonna need a couple of them, actually.

Conspirator-2: Let's get one up and working um they're [U/I] simple to build. Um let's get one up and working and make sure it's working correctly, you know we'll run it through its tests and um in the end yea, build as many as you want.

Conspirator-1: Alright.

Conspirator-2: Alright?

Conspirator-1: Alright cool.

Conspirator-2: We'll work on that as soon as I get back to uh Colorado.

11. Based on my training and experience, I have probable cause to believe that this call indicates that Conspirator-1 asked Conspirator-2 to build a Tor router, which would allow them to operate on the darknet, using a “razz pi,” which I believe refers to a “Raspberry Pi” (a type of computer) so that the defendant and Conspirator-1 could run their illegal website anonymously to evade law enforcement.

Conspiracy To Launder Drug Proceeds

12. Beginning in or around early 2021, law enforcement learned that the defendant, Conspirator-1, and Conspirator-2 (collectively, the “Co-conspirators”) conspired to launder proceeds derived from the original darknet drug conspiracy scheme that had not previously been discovered by law enforcement during those investigations.

13. As a result, federal law enforcement began listening in 2021 to lawfully recorded calls (“Jail Calls”) from the New Jersey state prisons where defendant and Conspirator-1 were incarcerated.

14. During this investigation, law enforcement has reviewed hundreds of Jail Calls and emails between the Co-conspirators discussing how the group used Bitcoin earned from the drug conspiracy in 2014 to purchase a cryptocurrency known as Ethereum (also referred to as “ETH”) in an Initial Coin Offering (“ICO”)², and how the ETH was now controlled by Conspirator-2 on Conspirator-1’s and the defendant’s behalf. They also discussed how to hide the cryptocurrency proceeds from law enforcement and how to reduce or eliminate any owed taxes. Finally, they discussed Conspirator-2’s “cut” of the ETH as a reward for managing the ETH while the defendant and Conspirator-1 are incarcerated.

15. Using various databases and open-source information, law enforcement has been able to trace the purchase of the ETH back to the ICO, indicating that it was purchased with 15 Bitcoin in July 2014, just as the Co-conspirators discussed. The ICO, though subscribed to in July 2014, delivered the proceeds of the 30,000 ETH to a wallet controlled by the defendant and Conspirator-1 on or about July 30, 2015. The 30,000 ETH was later transferred to a wallet controlled by Conspirator-2 on or about April 10, 2019.

16. In a Jail Call between Conspirator-1 and Conspirator-2 on or about September 11, 2018, for example, Conspirator-1 explained to Conspirator-2 how he and the defendant originally acquired the 30,000 ETH:

Conspirator-1: You, you, you, you, read that, um, blog post you sent me, right? The whole thing?

Conspirator-2: Yeah, why?

Conspirator-1: You saw how much ether they were handing out at initial offerings, right?

Conspirator-2: Um, I don’t remember what the number is but I know it was a fair amount.

² An “ICO” is a capital-raising event in which an entity offers investors a unique “coin” or “token” in exchange for consideration—most commonly in the form of established virtual or fiat currencies. These tokens are issued on a blockchain. To participate in an ICO, investors are typically required to transfer virtual currencies to the issuer’s address, online wallet, or other account. During an ICO, or after its completion, the issuer would typically distribute its unique “tokens” to the participant’s unique address on the related virtual currency’s blockchain. Similar to stockholders in an initial public offering (“IPO”), holders of a token are entitled to certain rights related to a venture underlying the ICO, such as profits, shares of assets, use of certain services provided by the issuer, and voting rights.

Conspirator-1: Two-thousand, the first offering was two-thousand for bitcoin.

Conspirator-2: Right.

Conspirator-1: And bitcoin was trading at about six hundred bucks a bitcoin.

Conspirator-2: Yeah, yeah.

Conspirator-1: So, remember I told you, we got ether at about thirty cents for ether?

Conspirator-2: Yeah, yeah.

Conspirator-1: That's how we came up with it. Because it cost, cost us about fifteen bitcoins.

Conspirator-2: Yeah, okay.

Conspirator-1: So. And bitcoin was raised (IA) six hundred dollars at that time.

17. Based on my training and experience, I believe Conspirator-1 is explaining to Conspirator-2 that Conspirator-1 and the defendant used approximately 15 bitcoins—then worth \$600 USD a bitcoin (for a total of \$9,000 USD worth of bitcoin)—to purchase 30,000 ETH. When Conspirator-1 states that “we got ether at about thirty cents per ether” he is explaining that \$9,000 worth of bitcoin divided by 30,000 ETH equals approximately thirty cents per ether. ($\$9,000 \text{ USD} \div 30,000 \text{ ETH} = \0.30 per ether.)

18. The object of the conspiracy was to conceal the true nature, location, source, ownership and control of the proceeds of the darknet drug conspiracy, and then launder those proceeds. The Co-conspirators agreed to engage in domestic and international transactions designed, in whole or in part, to conceal the nature, location, source, ownership and control of the proceeds, and agreed to engage in domestic and/or international transactions through cryptocurrency exchanges while making misrepresentations as to the source of the specified unlawful activity proceeds.

19. In an email dated March 11, 2021 from the defendant to Conspirator-1 that was sent through a third-party associated with Conspirator-1, the defendant discussed with Conspirator-1 how they would hide the source of the 30,000 ETH.

Defendant: In regards to proving the source of funds, when the coins

were acquired were talking like \$100-150k, right? I believe we could somehow prove the source of the funds. Even if you say it was your life savings. How can anyone say otherwise. Obviously, the coins have no transaction history since you put them in that wallet. On top of that by the time any of it comes under scrutiny it will be multiple years from now. The IRS will have to accept what you say because it will be like 8 or 9 years in the past. Don't you think? In that scenario it doesn't matter where the funds came from because its past any statute of limitations. The only fact on the table would be the coins were put in that wallet in like 2014 so at most the \$100k- 150k was the invested amount and everything over that is subject to capital gains.

20. In a Jail Call between the defendant and his then-girlfriend ("GF") on or about November 4, 2018, the defendant also explained how the Ethereum held by Conspirator-1 and the defendant was purchased with Bitcoin:

GF: There's a bitcoin address in the file.

Defendant: Yeah, but that's the address that when I... **When I bought this stuff, I bought it with bitcoin.**

GF: Okay.

Defendant: I didn't buy it with dollars. So, when I sent bitcoin, that's the address it came from. That was my bitcoin address.

(Emphasis added). Based on my training and experience, I have probable cause to believe that the defendant is referring to purchasing the Ethereum in the ICO using Bitcoin.

21. Between approximately 2018 and 2022, the Co-conspirators had numerous discussions about how they would sell the ETH, along with their other cryptocurrency holdings, once it reached a certain value. The focus of these conversations was frequently on how they could avoid drawing the attention of banks, exchanges, and law enforcement because of the illegal source of the Bitcoin used to purchase the ETH, and how they could avoid paying taxes.

22. For example, on or about July 12, 2021, Conspirator-2 expressed concern to Conspirator-1 about his potential criminal exposure should law enforcement find out about the money laundering scheme. He and Conspirator-1 discussed options to help protect Conspirator-2 until the defendant and Conspirator-1 were out of custody. Conspirator-2 stated that he was "all for" saving as much money as possible by, for example, moving the ETH to a

Bahamian corporation, but he wanted to make sure his exposure was limited in terms of “how much trouble a person could get in.”

23. In another Jail Call, on or about July 15, 2021, Conspirator-1 and Conspirator-2 again discussed shielding Conspirator-2 from the risk of being associated with illegal money laundering activity:

Conspirator-2: Okay, so the exit strategy is liquidation?

Conspirator-1: The exit strategy is liquidation and then if, if the time being comes repurchasing, you know what I’m saying.

Conspirator-2: Right.

Conspirator-1: But, but, but it would be minimal used. You know what I’m saying? It would be dormant most of the time and everything would be kept cold. All right?

Conspirator-2: All right.

Conspirator-1: And then, and then when the time being, when we come home, um, we could um, uh, what do you call it, uh, do everything personally with us, like, you wouldn’t have to be involved or anything like that, like, we’ll be doing all the running around and for something more, more permanent, you know what I’m saying?

Conspirator-2: Right.

Conspirator-1: Like think, like think, think of this like a burner phone, you know what I’m saying?

Conspirator-2: Okay, I’m with ya.

Conspirator-1: All right. So, um, and, and if any issues arises, it all links back to me and him. You know what I’m saying?

Conspirator-2: Okay.

24. On or about July 19, 2021, Conspirator-1 and Conspirator-2 discussed what would happen if an exchange became suspicious when they tried

to move the ETH overseas, reiterating that they believed as long as they could say the source of the ETH was the ICO, they could “sate” the exchanges.

25. During another Jail Call on or about June 21, 2022, Conspirator-1 and Conspirator-2 continued to discuss a plan to move the Ethereum overseas. Specifically, Conspirator-2 discussed how they could set up a domestic bank account even though the corporation they were creating to move the Ethereum would be international.

26. In or around June 2022, Conspirator-1 expressed concern about using publicly available computers in the jail to trade cryptocurrency and to make other financial trades. Accordingly, due to the risk of conducting transactions from the prison computers, Conspirator-2 controlled Conspirator-1 and the defendant’s Ethereum and other cryptocurrency holdings and kept cryptocurrency keys and wallets for accessing the defendant’s and Conspirator-1’s ETH at his residence in Colorado.

**Conspirator-2 to Receive 2,000 ETH for Managing Ethereum and Other
Cryptocurrency Held By the Defendant and Conspirator-1**

27. During lawfully recorded jail calls in March 2021, Conspirator-1 and Conspirator-2 discussed Conspirator-2’s compensation for managing Conspirator-1 and the defendant’s ETH and other cryptocurrency. On or about March 8, 2021, for example, Conspirator-1 and Conspirator-2 discussed the percentage of ETH that Conspirator-2 would be paid for the work he performed for the defendant and Conspirator-1 while they were in custody. Conspirator-2 suggested that he receive 10 percent of the Ethereum once they “cashed out.”

28. In an email from the defendant to Conspirator-2 dated March 29, 2021, the defendant offers Conspirator-2 a portion of the 30,000 ETH in return for helping to launder ETH.

Defendant: Hey [Conspirator-2], Here is an official email to make you feel better. Even though I give you my word I know sometimes you and [Conspirator-1] like something more official. I, Christopher Castelluzzo, agree to give you 2,000 ETH tokens (Two Thousand.) You can withdraw them whenever you wish and they are yours to do whatever you want. Enjoy and thank you for all you do for me.

29. On or about March 31, 2021, Conspirator-1 and Conspirator-2 discussed the counterproposal from the defendant — offering Conspirator-2 2,000 of the approximately 30,000 ETH held by the defendant and Conspirator-1. At the end of the call, Conspirator-1 said he agreed with the defendant’s counteroffer and Conspirator-2 accepted it, saying “this makes me very happy.”

On or about March 31, 2021, 2,000 ETH was worth approximately \$3.69 million.

Cryptocurrency Seized From Conspirator-2 July 12, 2022

30. On or about July 12, 2022 law enforcement executed a search warrant at the residence of Conspirator-2 in Colorado. Seized from a computer at Conspirator-2's residence during the execution of the search warrant were electronic wallets containing various cryptocurrency controlled by the Co-conspirators, including the approximately 30,000 ETH.

Conclusion

31. I submit there is probable cause that the defendant conspired to engage in financial transactions designed in whole and in part to conceal and disguise the nature, location, source, ownership and control of proceeds of specified unlawful activity, to wit, conspiracy to distribute and the distribution of controlled substances, while knowing that the source of the funds was from some form of unlawful activity.