

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

UNITED STATES OF AMERICA

v.

JAMES WAN,

Defendant.

CRIMINAL ACTION NO.

1:22-cr-188-LMM-CMS

FINAL REPORT & RECOMMENDATION

Defendant James Wan is charged with knowingly using a facility of interstate commerce with the intent that a murder be committed in consideration for payment, in violation of 18 U.S.C. § 1958(a). [Doc. 10].

On May 15, 2023, Wan filed a “Motion in Limine to Exclude and Suppress,” in which he complains that all of the evidence against him was obtained after the FBI received an anonymous tip, and he seeks to exclude “the uncorroborated unanimous (sic) tip” and the “voluntary confessions” he made to the federal agents as a result of that tip. [Doc. 37 at 1]. The Government filed a response, arguing that agents are permitted to question suspects about tips, and that there was nothing unlawful about the agents’ conduct that would require suppression. [Doc. 39]. Wan filed a reply brief, reiterating his belief that the agents acted improperly by

interviewing him because their facts were based on an “uncorroborated anonymous tip.” [Doc. 40 at 2–3].

I. Factual Background

In its response brief, the Government provided details regarding the background of the case, and Wan has not disputed the Government’s recitation. As such, I will accept the Government’s representations, and will quote directly from the Government’s brief to provide the factual background. According to the Government:

On May 11, 2022, the FBI received a tip from a confidential source who was known to the FBI and had previously provided accurate information. The source told the FBI that someone with username “jwan6725241” had solicited murder-for-hire services via a dark web marketplace (hereinafter, the “DWM”). According to the tip, the user had placed an “Order” on the DWM to have a specific person, hereinafter referred to as “the Victim,” killed in exchange for payment in bitcoins and had provided the Victim’s address in Duluth, Georgia. The tip further indicated that the user had already made two Bitcoin payments worth approximately \$16,000 total to the DWM on April 18 and 21, 2022.

Although agents believed the DWM was a scam with no actual hitmen, they remained concerned the user would try to have the Victim killed another way, so they traced the two identified Bitcoin payments and discovered they originated from a Coinbase digital wallet. Agents then requested and received information from Coinbase about the wallet. The information from Coinbase established that the wallet

belonged to Wan and showed he had recently made four Bitcoin payments, including the original two identified as going to the DWM:

- April 18, 2022 - \$7,960.85
- April 21, 2022 - \$7,998.66
- April 29, 2022 - \$7,712.79
- May 10, 2022 - \$1,235.66

Agents also conducted open-source searches on Wan and the Victim and discovered that they shared a young daughter, appeared to be in a romantic relationship, and lived together at the address listed in the Order.

On May 14, 2022, agents learned the Victim and Wan were at Northside Hospital Gwinnett in Lawrenceville, Georgia, where Wan was receiving treatment for broken ankles. Agents went to the hospital and interviewed the Victim. She confirmed her home address and explained that she had been dating Wan for the past nine years and that they had a daughter together. She further explained that she and Wan had been arguing for the past few months and that their relationship was not on good terms. She also told agents that she had recently reported Wan to his work for drinking in his office with coworkers. After learning about the possible threat to her, the Victim remembered some odd things Wan had recently done, including taking a video of her car and zooming in on the license plate. She also remarked that Wan had a private, locked browser on his phone called an “Onion browser” that could only be accessed with facial recognition. She also told agents that Wan had previously threatened to shoot her during an argument. After the interview, law enforcement took the Victim to a safe location.

Agents then interviewed Wan at the hospital and informed him that he was not in custody or under arrest. During the interview, Wan confirmed that he and the Victim had been arguing for the past six to eight months and that it had made him very angry when the Victim reported him to his work for drinking in the office because it threatened his career and livelihood. Agents told Wan that they heard Wan posted something seeking to hurt the Victim, and they asked him whether he

had ever been on the dark web and had a Coinbase account. Wan denied having ever accessed the dark web but acknowledged he had a Coinbase account. Agents then told Wan that one transaction traced back to his Coinbase account, and Wan suggested that maybe he had been hacked. Agents explained that they were going to go back and look at who accessed the DWM site and urged Wan to tell the truth, saying at one point, “if it was a mistake, it was a mistake.” Shortly thereafter, Wan admitted that he “made the mistake.”

At that point, although Wan was still not in custody, agents read him his *Miranda* rights, and he agreed to speak with the agents further without a lawyer present. When asked how much he paid to the DWM hitman site, Wan explained that he made four Bitcoin payments worth approximately \$7,500, \$7,500, \$7,500, and \$5,000. The first disappeared from his “escrow” account on the site, and he believed someone had scammed him out of that payment. The second two payments were intended to reach the \$15,000 required to hire a hitman, and the last payment was to top off the account after the value of Bitcoin fell. Wan then explained that he had checked the DWM hitman site daily after placing the Order. Wan consented to agents searching his phone, which he did not have with him at the hospital. Wan also suggested he could cancel the Order and withdraw all his funds from the escrow account if agents brought him his phone. Agents left Wan at the hospital without arresting him.

On May 17, 2022, agents returned to the hospital with Wan’s iPhone. While agents watched and recorded him, Wan voluntarily accessed the DWM hitman site from his iPhone. After opening the Onion Browser application on his iPhone via facial recognition and logging into the DWM with username “jwan6725241” and his password, WAN [sic] showed agents the Order, which identified the Victim by name (first and last), provided her home address, described her car and license plate, and stated, “Can take wallet phone and car. Shoot and go. Or take car.” The “Status” of the order showed as, “Payment submitted and secured in escrow.” After accessing his Coinbase account to obtain his Bitcoin wallet address, Wan requested

a refund of the funds in his escrow account on the DWM and cancelled the Order. Agents again left Wan at the hospital without arresting him.

On May 19, 2022, agents again returned to the hospital with Wan's iPhone. While agents again watched and recorded him, Wan voluntarily accessed the DWM to confirm that the Order had been canceled. No active Order appeared on Wan's account, but the bitcoins still appeared to be in his escrow account, so he again requested a refund. Wan also showed agents two questions he had posted on the site's forum tab. The first, dated May 2, 2022, stated, "I have submitted an order and curious how quickly it should be carried out? Is there a way I can find out any progress? If there is anyone in my location?" The second, dated May 5, 2022, stated, "I've contacted admin. I need this taken care of fast. Who can help. Duluth, ga. USA." Wan also showed agents two messages he had sent to the site administrator. The first, dated May 11, 2022 (which was the day after he made his final Bitcoin payment to the site), identified the Victim by name (first and last) on the subject line and stated, "This is all I have. I only wanted to spend \$15000." The second, dated May 12, 2022, again identified the Victim by name (first and last) on the subject line and stated, "Thanks. How soon do you think it can be done. This weekend? We have a court date Tuesday 17. It would be good if it could be done before the 17." Agents again left Wan at the hospital without arresting him.

The following day, May 20, 2022, agents arrested Wan pursuant to [a] federal criminal complaint and arrest warrant signed by U.S. Magistrate Judge Linda T. Walker. And on May 24, 2022, a grand jury indicted Wan for knowingly using a facility of interstate commerce with the intent that the murder of the Victim be committed in consideration for payment, in violation of 18 U.S.C. § 1958(a).

[Doc. 39 at 2–7] (footnotes omitted).

In his motion, Wan argues that statements he made to the FBI at the hospital should be suppressed because that evidence "was gathered as a result of an anonymous tip that was uncorroborated." [Doc. 40 at 3; *see also* Doc. 37 at 1]. He

argues that his confession amounts to “fruit of the poisonous tree” and should be suppressed, citing *Lawson v. State*, 684 S.E.2d 1 (Ga. App. 2009), *United States v. Timmann*, 741 F.3d 1170 (11th Cir. 2023), and *Utah v. Strieff*, 579 U.S. 232 (2016). [Doc. 37 at 2; Doc. 40 at 3].¹

I previously addressed the issue of the identity of the tipster during a pretrial conference in which we discussed Wan’s Motion to Reveal the Identity of Informants. [Doc. 30; Doc. 41, Transcript (“Tr.”)]. During that conference, the Assistant United States Attorney revealed that a news organization provided the tip. [Tr. at 3–4]. The AUSA stated that the news organization “passively” saw the request for a hitman, considered it to be a credible threat, and then reported it to the FBI; that this was not any kind of sting operation or police trap; that the source did not communicate with Wan in any way; and that the Government had an important

¹ Wan also argues for the first time in his reply brief that the agents obtained certain information from Coinbase without probable cause. [Doc. 40 at 2]. Wan, however, provides no specifics regarding (1) what particular information he is referring to; (2) how the agents obtained this information (i.e., by subpoena, warrant, etc.); or (3) what the legal basis for his challenge might be. [*Id.*]. Because Wan did not raise this issue in his original brief and did not thereafter provide any factual or legal support for it, I find that this argument is without merit.

interest in not disclosing more information about the organization in order to protect the source for future investigations. [*Id.* at 3–4, 9].

Pursuant to *Roviaro v. United States*, 353 U.S. 53 (1951), the Government has the privilege to withhold the identity of an informant unless the informant’s information is “relevant and helpful to the defense of an accused.” 353 U.S. at 61–63. During the pretrial conference, the Government argued that the information from the informant would not be used to build the case and that the information from the informant was not exculpatory. Based on the AUSA’s representations, I ruled that the Government could withhold the informant’s identity, and I refused to conduct an in camera review of the information surrounding the tip. [*Id.* at 6–7]. Wan did not appeal that ruling.

In the instant motion, Wan persists in his erroneous contention that the tip was anonymous, and he now argues that any “evidence gathered as a result of the anonymous tip . . . is tainted and must be suppressed.” [Doc. 37 at 2]. This argument is flawed both factually and legally.

As noted above, the tip was not anonymous; rather, it was provided by a news organization. But even if the tip were anonymous, the argument would still fail because Wan has pointed to no misconduct on the part of the agents that might taint his confession. Wan provides no legal authority for his contention that the


Government is not allowed to follow up on tips it receives—anonymous or otherwise. On the contrary, consensual encounters like those between Wan and the agents at the hospital do not even implicate the Fourth Amendment. *See United States v. Jordan*, 635 F.3d 1181, 1185-86 (11th Cir. 2011).

Here, agents properly confronted Wan during consensual encounters and asked him about information they had obtained lawfully, i.e., a tip they received from a news organization (who was known to the FBI and had previously provided accurate information) and corroborating information they legally obtained from their trace of the Bitcoin payments, Coinbase, open-source searches, and the Victim. In the absence of any illegality that could have tainted Wan’s confessions and admissions, the fruit of the poisonous tree doctrine is inapplicable. *See United States v. Prunick*, No. 1:06-cr-179-ODE-LTW, 2006 WL 8448759, at *9 (N.D. Ga. Nov. 16, 2006) (noting that where there is no poisonous tree to begin with, any evidence seized during a consent search cannot be fruit of such a tree), *adopted by* 2007 WL 9758001 (N.D. Ga. Feb. 23, 2007); *see also United States v. Masse*, 816 F.2d 805, 810 (1st Cir. 1987) (rejecting a fruit-of-the-poisonous-tree argument where “there was no primary illegality to taint [the] subsequent statements”). Accordingly, Wan

has failed to show that there are any grounds to suppress or exclude Wan's statements to the FBI agents.

For the reasons stated, I **RECOMMEND** that Wan's Motion in Limine to Exclude and Suppress [Doc. 37] be **DENIED**. There are no other pending matters before me in this case. Accordingly, Wan's case is hereby **CERTIFIED** ready for trial.

This 10th day of July, 2023.



CATHERINE M. SALINAS
United States Magistrate Judge