U.S. Department of Justice

United States Attorney
Southern District of New York

The Silvio J. Mollo Building
One Saint Andrew's Plaza
New York, New York 10007

February 15, 2023

BY ECF

Honorable Lewis A. Kaplan
United States District Judge
Daniel Patrick Moynihan
United States Courthouse
500 Pearl Street
New York, NY 10007-1312

Re: *United States v. Samuel Bankman-Fried*, 22 Cr. 673 (LAK)

Dear Judge Kaplan:

The Government writes to request that the Court modify the defendant's conditions of pretrial release to limit his use of cellphones, tablets, computers, and the internet. Within the span of a month, the defendant has used at least two methods of encryption in a manner that warrant modification to his bail conditions. His behavior shows that the existing conditions leave too much room for circumvention of restrictions aimed at preventing inappropriate conduct, including contacting witnesses and accessing cryptocurrency assets. Because the defendant is a technologically sophisticated person with both the ability and the inclination to seek workarounds of more narrowly drawn bail conditions, the Court should, for the reasons set forth below, (i) prohibit the defendant's use of cellphones, tablets, computers, and the internet except for the limited uses and subject to the conditions set forth below; (ii) prohibit the use of all other cellphone and computer call and messaging applications; (iii) require the installation of a device monitoring program on the defendant's cellphone and computer; and (iv) require pen registers on the defendant's cellphone number and Gmail account.

I. Background

On December 22, 2022, the defendant was released on bond. On January 15, 2023, the defendant contacted a potential witness at trial, without the presence of either the defendant's or the witness's counsel. (Dkt. 58 at 3.) The defendant contacted the witness through the encrypted messaging application Signal, as well as by email, and wrote in relevant part that he would "really love … for us to have a constructive relationship, use each other as resources when possible, or at least vet things with each other." (*Id.*) As the Court described previously, "the message in its entirety seems to be an invitation for [the witness] to align his views and recollection with defendant's version of events and thus make their relationship "constructive." (*Id.* at 5.) After the Government brought the message to the Court's attention, the Court preliminarily amended the conditions of the defendant's release to add the conditions that "(1) the defendant shall not contact

or communicate with current or former employees of FTX or Alameda (other than immediate family members) except in the presence of counsel, unless the government or Court exempts an individual from this rule and (2) the defendant shall not use any encrypted or ephemeral call or messaging application, including but not limited to Signal." (*Id.* at 6-7.)

At a conference on February 9, 2023, the Court raised concerns that, even with the parties' proposed new bail conditions, the defendant could continue to encrypt and delete certain data from applications on his phone. The Court noted: "We are being a little shortsighted by focusing only on apps." (Feb. 9, 2023 Tr. at 6.) After hearing from the parties on the proposed modifications to the conditions of release, and noting what the Court described as "a very real risk of misuse" by the defendant of his devices, the Court extended the February 1, 2023, order to and including February 21, 2023. (Feb. 9, 2023 Tr. at 10.) The Court also permitted the parties to make submissions by February 13, 2023, to propose conditions, including a technical solution, that would address the issues raised by the Court. Shortly after the conference, the parties began discussing proposals to address the concerns raised by the Court.

On February 13, 2023, it came to the Government's attention, based on data obtained through the use of a pen register on the defendant's Gmail account, that the defendant has used a VPN or "Virtual Private Network" on at least two occasions to access the internet. A VPN hides a user's IP address by letting the private network redirect it though a remote server run by the VPN's host. In particular, the Government was alerted to the issue because while it appears that the defendant was typically logging into his email account using the internet service in his parent's house, on two occasions there appeared to be logins from Singapore. The defendant, of course, was not in Singapore, but the pen registered captured IP addresses that might have otherwise suggested that the individual logging in to the defendant's email account was not in the United States.

That same day, the Government alerted defense counsel to the defendant's use of a VPN. While defense counsel did not deny the defendant's use of a VPN, counsel suggested that the use of a VPN related to the defendant's preparation of his defense and defense strategy and a need to access web content not otherwise available within the United States. The Government then raised the VPN usage with the Court by letter, requesting more time to consider and discuss the conditions of release. By letter dated February 14, 2023, defense counsel noted that "on the specific dates referenced by the Government, [the defendant] used the VPN to access an NFL Game Pass international subscription that he had previously purchased when he resided in the Bahamas, so that he could watch NFL playoff games"—specifically the AFC and NFC Championship games on January 29, 2023, and the Super Bowl on February 12, 2023. (Dkt. 67.) An international subscription to NFL Game Pass was not necessary to watch the Super Bowl; it was, for instance, on cable TV, free over the air using an antenna, viewable on the Fox Sports app for free, and also was streamed in the U.S. on some secondary websites.[1] The letter also did not address whether the defendant has used a VPN on other occasions and for other purposes that did not involve logging into his email account, such that the Government would have no evidence of the defendant's VPN use.

---

[1] https://www.cnet.com/tech/services-and-software/watch-super-bowl-2023-today-for-free-online-start-time-tv-network-and-streaming/.

II. The Court Should Modify the Terms of Pretrial Release

Section 3142(c)(3) of the Bail Reform Act permits the Court to amend the order releasing a defendant on pretrial conditions "to impose additional or different conditions of release [at any time." 18 U.S.C. § 3142(c)(3). Courts may amend a release order under section 3142(c) where there is a changed situation or new information that warrants alerted release conditions. (Dkt. 58 at 4.)

The defendant's contact with a possible trial witness in January 2023 using Signal, and the defendant's use of a VPN after the Court already restricted the defendant's use of encrypted messaging applications, are a sufficient basis to warrant the imposition of additional conditions of release. The Court previously observed—correctly—that the defendant's contact with a prospective witness using Signal justified imposition of additional bail conditions, and that access to multiple cellphone applications that are encrypted or permit deletion create a continuing risk of misuse. (*Id.*; *see also* Feb. 9, 2023 Tr. at 11.) While the Government was working with defense counsel on an appropriately restrictive condition on the use of cellphone and computer applications, the defendant's recently discovered use of a VPN, and his unsatisfactory explanations for its use, confirms the Court's intuition that "focusing only on apps" is "shortsighted" (Feb. 9, 2023 Tr. at 7), and justifies considerably more restrictive conditions.

From the standpoint of pretrial supervision, the use of a VPN is problematic. It is a mechanism of encryption, hiding online activities from the Government. That is of particular concern since the issue around the defendant's conditions of release arose from the defendant's use of Signal—an encrypted cellphone application—for purposes of evading law enforcement detection. Additionally, a VPN is a means to disguise a user's whereabouts because a VPN server essentially acts as a proxy on the internet.

More fundamentally, the use of a VPN highlights that the previously proposed conditions are insufficient to restraint a technologically sophisticated individual, like the defendant, with the will to circumvent detection and monitoring. The defendant used a VPN *after* the Court expressed concern about the use of encrypted channels beyond those identified by the Government in its proposed bail conditions, and once he was already on notice about the Government's concerns regarding encrypted and undetectable electronic activity. Even assuming that on those occasions the defendant was watching football that was otherwise available for viewing in the United States, the possibility and likelihood remain that the defendant has used a VPN more often, and for purposes besides watching football, that the Government was simply unable to uncover. The Court therefore cannot be reassured that the defendant will not exploit the Government's failure to anticipate alternative means of encryption and covert internet usage. That is illustrated by what happened here: while the Government's attention was directed toward encrypted communication channels, unbeknownst to the Government, the defendant was simultaneously using a VPN.

By changing IP addresses through a VPN, the defendant would be able to undermine attempts by law enforcement to monitor his activity to ensure that he is not inappropriately contacting witnesses. Moreover, the use of a VPN poses serious risks beyond witness tampering. As the Court recalls, in January the Government asked for a condition prohibiting the defendant

from transferring FTX and Alameda Research funds after evidence emerged on the blockchain that cryptocurrency was being transferred from digital wallets that belonged to Alameda Research to crypto mixers and other exchanges. The Government commenced an investigation, but did not find evidence connecting the cryptocurrency transfers to the IP address associated with the internet service that the defendant was using from his parent's home in Stanford, California. But the recent discovery of the defendant's use of a VPN means that the Government cannot presently rule out that those transfers were, in fact, by the defendant—who once had access to the keys to those wallets and who we now know has been using a VPN that makes it appear as though his internet activity is being conducted by someone in Asia or elsewhere. The use of a VPN also theoretically gives the defendant the ability to access cryptocurrency exchanges that block IP addresses associated with the United States, which would allow him to conduct cryptocurrency transactions without detection by law enforcement.

To be sure, there is nothing illegal about using a VPN. But the defendant's usage—even if occasionally for benign reasons—makes pretrial supervision untenable for the reasons described herein. The solution is not simply to give the Government the defendant's IP addresses or prohibit the use of a VPN. There is now a record before the Court of a defendant who appears motivated to circumvent monitoring and find loopholes in existing bail conditions. The appropriate course, therefore, is broader restrictions on the defendant's cellphone, tablet, computer, and internet usage, with limited exceptions. The Government therefore proposes the following:

1. The defendant shall be prohibited from using cellphones, tablets, computers or the internet except for the limited uses and subject to the conditions set forth below.

2. The defendant is permitted to use electronic devices for purposes of reviewing discovery.

3. The defendant is permitted to use email through his Gmail account, and voice calls and SMS messages through his cellphone.

4. The defendant shall be permitted to use Zoom solely for communicating with his counsel.

5. The defendant shall be prohibited from using any other cellphone and computer call and messaging applications.

6. The defendant shall be limited to use of one cellphone and one computer, and both devices will have a device monitoring program installed by pretrial services.

7. The defendant's Gmail account and his cellphone number will be monitored through the installation of pen registers.

8. The defendant must submit his electronic devices to a search on the basis that the Probation Officer has a reasonable suspicion that evidence of a violation of a condition of release may be found.

Such conditions have been ordered in this District when a defendant has used computers to commit charged offenses, and there is a reason to believe he will continue to do so in the future. In particular, restrictions on the use of computers, cellphones, and the internet are appropriate when a defendant has attempted to circumvent bail restrictions, attempts to commit obstruction, or may continue the commission of criminal acts. *See, e.g.*, *United States v. Yin*, 15 Cr. 706-04 (S.D.N.Y. Nov. 5, 2015) (Dkt. Nos. 102, 407) (in a foreign bribery case, prohibiting the use of cellphones, and permitting the possession of a computer for limited purposes and with monitoring software installed); *United States v. Sharma*, 18 Cr. 340 (S.D.N.Y. May 11, 2018) (prohibiting use or access of any computer, smartphone, or the internet in securities fraud case where the defendant was suspected of attempting to tamper with witnesses). The proposed conditions would still permit the defendant to communicate with his counsel, review discovery, prepare for trial, and exercise his First Amendment rights, while being narrowly tailored to prevent violations of the conditions of release.

For these reasons, the Court should modify the conditions of release to impose the new restrictions set forth herein. For the reasons previously briefed, the Court should leave in place the bail conditions the Court already imposed regarding not contacting witnesses and not transferring funds or assets.

Respectfully submitted,

DAMIAN WILLIAMS
United States Attorney

by: /s/ Nicolas Roos
Nicolas Roos
Danielle R. Sassoon
Samuel Raymond
Thane Rehn
Andrew Rohrbach
Danielle Kudla
Assistant United States Attorneys
(212) 637-2421

Cc: Defense Counsel (by ECF)