UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA	:	
	:	
v.	:	**Criminal No. 21-cr-399 (RDM)**
	:	
ROMAN STERLINGOV,	:	
	:	
Defendant.	:	

GOVERNMENT'S REPLY IN SUPPORT OF NOTICE AND MOTION *IN LIMINE* TO ADMIT EVIDENCE AS INTRINSIC EVIDENCE OR, IN THE ALTERNATIVE, AS EVIDENCE OF OTHER CRIMES OR ACTS PURSUANT TO FEDERAL RULE OF EVIDENCE 404(b)

The United States of America, by and through the United States Attorney for the District of Columbia, respectfully submits the following Reply in support of its notice and motion *in limine* to admit evidence as intrinsic evidence or, in the alternative, as other crimes or acts evidence pursuant to Fed. R. Evid. 404(b), ECF No. 63.

ARGUMENT

As explained in the government's motion, the government intends to offer evidence relating to several topics, including (A) the defendant's use of and knowledge of Tor, Silk Road, and other Darknet markets, and the defendant's recreational drug use; (B) the defendant's technical knowledge and programming ability; (C) the defendant's use of aliases and efforts to conceal his identity and assets; (D) the defendant's operation of servers in Romania purportedly for a VPN service called "MoonVPN"; (E) the defendant's efforts to acquire BlindBitcoin; and (F) the defendant's efforts to set up other cryptocurrency projects. Most if not all of the above-described evidence is properly considered intrinsic because it represents direct evidence of the Bitcoin Fog scheme and the defendant's efforts to conceal his activities. Out of an abundance of caution, the government also provided notice and moved for the admission of the six categories of evidence under Rule 404(b) for purposes other than character evidence. *See generally* ECF No. 63. The defendant opposes only certain kinds of evidence within the first four categories listed above; he does not oppose introduction of any of the evidence described in categories (E) or (F).

A. Defendant's Use of and Knowledge of Tor, Silk Road, and other Darknet Markets, and Defendant's Recreational Drug Use

1. Darknet Sites Involving Child Sexual Abuse Material or Assassination Market

The defendant disputes (at 6-7) the admission of evidence showing Bitcoin Fog's transactions involving the darknet "Assassination Marketplace" site or child sexual abuse material darknet sites, based on the "prejudicial" nature of such evidence.[1] If anything, this appears to be an argument about admissibility under Rule 403 and not a claim about improper purpose under Rule 404(b). But as the government explained in its opposition to the defendant's Rule 403 argument in his omnibus motion *in limine*, evidence that Bitcoin Fog processed transactions to facilitate such illegal marketplaces is *directly* relevant to core elements of the charged offenses—including the existence of a conspiracy between the defendant, as operator of Bitcoin Fog, and "darknet vendors and darknet administrative teams," ECF No. 43, at 1-2; and whether Bitcoin Fog transmitted funds known to have been "derived from a criminal offense" or "intended to be used to promote and support unlawful activity," *id.* at 4. *See* ECF No. 73, at 37-40.

To be sure, evidence related to the sexual exploitation of children or assassination markets is likely to be distressing to jurors. But that is not the standard for admissibility, which tilts in

[1] In his opposition to the government's Rule 404(b) Notice, the defendant does not contest admission of evidence relating to drug trafficking darknet sites like Silk Road or Agora, as raised in the government's filing. However, in the defendant's Omnibus Motion *in Limine*, he does raise a cursory objection to "evidence discussing Silk Road, Agora, or any other online criminal marketplace" under Rules 401, 403, and 404. ECF No. 59, at 5, 8-9. The government addressed the defendant's objection in its response, *see* ECF No. 73, at 37-40, and incorporates those argument by reference here.

favor of admission unless the risk of unfair prejudice "*substantially* outweigh[s]" the probative value of the evidence. Fed. R. Evid. 403 (emphasis added). In this case, one of the elements of Count Three, on which the government bears the burden of proof, is that Bitcoin Fog processed transactions involving funds either "derived from a criminal offense" or "intended to be used to promote and support unlawful activity." ECF No. 43, at 4. Evidence that Bitcoin Fog processed transactions for child sexual abuse material, illegal drug trafficking, or any other illegal service is direct and highly probative evidence of this element. Nor is it *substantially* and *unfairly* prejudicial. Whatever prejudice there may be, it is related to the defendant's *own* crimes: by operating a bitcoin money laundering service designed to make darknet transactions untraceable, the defendant in fact contributed to the enormous harm and suffering created by these illegal sites. The government has a right to introduce direct evidence of the offenses in the Superseding Indictment, even if such evidence is unavoidably prejudicial. *See Old Chief v. United States*, 519 U.S. 172, 186 (1997) ("[T]he prosecution is entitled to prove its case by evidence of its own choice . . . .").[2]

The defendant's only other argument (at 7) is that the government has not proven the defendant's "connection" to Bitcoin Fog, but this is a disagreement with the weight of government's evidence and not an argument about relevance or improper purpose.

2. Knowledge and Use of Tor

The defendant also disputes (at 8-9) whether the defendant's knowledge and use of Tor is relevant because it does not, by itself, prove that the defendant operated Bitcoin Fog. But the test of relevance is only whether the evidence tends to make any material fact more or less probable.

[2] The government does not intend to introduce graphic exhibits such as images of the child sexual abuse material found on the illegal sites serviced by Bitcoin Fog, but only to describe the child sexual abuse material available on these sites through text records and witness testimony.

See Fed. R. Evid. 401 advisory committee notes ("A brick is not a wall[.]"). The fact that the defendant had the Tor browser installed on his electronic devices and that he instructed associates on how to access Tor and Silk Road may not be conclusive, but it is certainly relevant to (a) whether the defendant himself operated a Tor-based service, Bitcoin Fog; and (b) whether he had knowledge that sites like Silk Road facilitated drug trafficking transactions—which goes to his knowledge that Bitcoin Fog engaged in transactions involving the proceeds of drug trafficking offenses by processing transactions from Silk Road and similar sites. *See* ECF No. 43, at 2 (citing knowledge elements of 18 U.S.C. § 1956(a)(1)(A)(i) and (a)(1)(B)(i)), 4 (citing knowledge element of 18 U.S.C. § 1960(b)(1)(C)). The government is entitled to introduce evidence related to the knowledge element of the charged offenses. *United States v. Mosquera-Murillo*, 153 F. Supp. 3d 130, 183-84 (D.D.C. 2015) ("[W]here the government is required to demonstrate as an element of a charged offense a defendant's intent and knowledge, admission of other crimes evidence is permissible even where the defendant has not affirmatively challenged these elements.").

The defendant also notes that the Tor network was originally created by the U.S. government and has legitimate uses. That does not undermine the probative value of any of the evidence described above, but it does show that it poses little risk of unfair prejudice under Rule 403.

B. Defendant's Technical Knowledge and Programming Ability

The defendant argues (at 2, 9-10) that evidence of the defendant's technical ability is irrelevant because the government has not connected the defendant's specific skills to the particular "network architecture" of Bitcoin Fog. Again, that argument confuses relevance with a disagreement about the weight of the evidence. And even at a high level of generality, the fact that the defendant has sophisticated programming skills, managed a remote server (the "MoonVPN" server), and operated a Bitcoin client capable of sending and receiving bitcoin transactions all tends to make it more probable that he had the technical knowledge, intent, preparation, and plan with respect to Bitcoin Fog.

The defendant is also mistaken in claiming (at 2) that the government has not offered evidence of the Bitcoin Fog's "network architecture" or "what type of code it use[d]." As described in the government's opening motion, the government identified an outgoing message from the shortmint@hotmail.com email account associated with Bitcoin Fog in which the sender, identifying himself as "Akemashite," describes his *own* programming skill set: "I am a proficient developer in C/C++ (mostly for windows platform, but many of the libraries I used are platform-independent), Java, PHP, Python, HTML/CSS, JS." *See* ECF No. 63, at 9. That is direct evidence of the programming skill set used to create Bitcoin Fog. Separately, the fact that the language of Akemashite's self-description closely parallels the language used by the defendant in one of his attributable email accounts, heavydist@gmail.com, supports the conclusion that Akemashite and the defendant are the same person.

C. Defendant's Use of Aliases and Efforts To Conceal Identity and Assets

The defendant disputes (at 10) the government's evidence relating to the defendant's use of aliases and online monikers because, he claims, the government has not "connected" these aliases with the defendant. As noted above, this is a disagreement with the weight of government's evidence establishing the connection between these aliases and the defendant; it is not an argument about relevance or improper purpose.[3]

[3] The defendant also mistakes the significance of the Internet Protocol (IP) address evidence in this case. The government is not asserting that IP addresses by themselves count as "Personally Identifiable Information," as the defendant inaccurately states (at 10). Instead, the significance

The defendant does not dispute the admissibility of evidence relating to the defendant's other efforts to conceal his assets, such as purchasing untraceable gold or using Bitcoin Fog to conceal his own assets.

D. Defendant's MoonVPN Servers

The defendant argues (at 11) that evidence relating to the defendant's servers in Romania, which the defendant allegedly operated in the name of a Virtual Private Network (VPN) service called "MoonVPN," and which he also used to run Bitcoin client software, is "irrelevant." But the government has explained how evidence related to the Romanian servers is relevant (1) to show the defendant's efforts to launder Bitcoin Fog proceeds through MoonVPN accounts, and (2) to show the defendant's sophistication and technical ability in creating complex code, using and managing remote server infrastructure, and operating a Bitcoin client capable of sending and receiving bitcoin transactions. ECF No. 63, at 11-12. The defendant's conclusory denial does not address either argument.

The defendant also argues that evidence related to the Romanian servers could confuse the jury. The government anticipates that the evidence and testimony regarding these servers should be sufficiently clear; and the defense will have an opportunity to draw out any factual distinctions through cross-examination of the government's witnesses. To the extent jury confusion remains a concern, it should be addressed through an appropriate limiting instruction. *E.g.*, *United States v. Glover*, 583 F. Supp. 2d 5, 16 (D.D.C. 2008) (finding that "limiting instructions" would be sufficient to avoid risk of jury confusion in complex co-defendant drug trafficking case).

lies in the coincidence of two things close in time—the fact that a given IP address was used to access accounts and aliases associated with Bitcoin Fog and was also used in the same time frame to access attributable accounts belonging to Roman Sterlingov—which supports a conclusion that the same individual was accessing both accounts through a common Internet connection.

CONCLUSION

For the foregoing reasons, the Court should grant the government's *motion in limine* to admit the evidence described in the motion as intrinsic evidence and/or evidence of other crimes or acts pursuant to Fed. R. Evid. 404(b).

Respectfully submitted,
MATTHEW M. GRAVES
UNITED STATES ATTORNEY
D.C. Bar No. 481052

BY: */s/ Christopher B. Brown*
Christopher B. Brown, D.C. Bar No. 1008763
Assistant United States Attorney
U.S. Attorney's Office for the District of Columbia
601 D Street, N.W.
Washington, D.C. 20530
(202) 252-7153
Christopher.Brown6@usdoj.gov

/s/ C. Alden Pelker
C. Alden Pelker, Maryland Bar
Trial Attorney, U.S. Department of Justice
Computer Crime & Intellectual Property Section
1301 New York Ave., N.W., Suite 600
Washington, D.C. 20005
(202) 616-5007
Catherine.Pelker@usdoj.gov