UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

– v. –

KEONNE RODRIGUEZ and
WILLIAM LONERGAN HILL,

Defendants.

S3 24 Cr. 82 (DLC)

THE GOVERNMENT'S SENTENCING MEMORANDUM REGARDING DEFENDANTS KEONNE RODRIGUEZ AND WILLIAM LONERGAN HILL

NICOLAS ROOS
Acting Deputy United States Attorney
Attorney for the United States
Acting Under Authority Conferred by
28 U.S.C. § 515
26 Federal Plaza, 37th Floor
New York, New York 10278

Andrew K. Chan
David R. Felton
Cecilia E. Vogel
Assistant United States Attorneys
- Of Counsel -

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

– v. –

KEONNE RODRIGUEZ and WILLIAM LONERGAN HILL,

Defendants.

S3 24 Cr. 82 (RMB)

GOVERNMENT'S SENTENCING MEMORANDUM REGARDING DEFENDANTS KEONNE RODRIGUEZ AND WILLIAM LONERGAN HILL

The Government respectfully submits this memorandum in advance of the sentencings of Defendants Keonne Rodriguez and William Lonergan Hill, which are respectively scheduled for November 6, 2025 at 11:00 a.m. and November 7, 2025 at 11:00 a.m.

I. PRELIMINARY STATEMENT

For nearly a decade, Rodriguez and Hill owned and operated a massive money laundering service known as "Samourai Wallet" ("Samourai"), which laundered millions of dollars in criminal proceeds on behalf of its customers. To generate revenue, boost Samourai's business, and earn millions of dollars in fees, Rodriguez and Hill repeatedly solicited, encouraged, and invited criminals to use Samourai to conceal their transfers of criminal proceeds—ultimately resulting in large-scale money laundering and sanctions evasion. In his sentencing letter, Hill himself admits that inviting "computer hackers and other criminals" to launder their crime proceeds through Samourai "spiraled well beyond acceptable limits." (Hill Letter at 3).[1] As a direct result of

[1] The Hill Letter begins at Dkt. 155 at 104.

Rodriguez and Hill's solicitations of criminals, at least $237 million in proceeds from drug trafficking, darknet marketplaces, cyber-intrusions, frauds, murder-for-hire schemes, and a child pornography website were laundered using Samourai. That laundering activity was not a byproduct; it was a feature. And it reflected Rodriguez and Hill's plan for Samourai Wallet from the outset. At its inception, the defendants intended for Samourai to be used to "wash" crime proceeds, and they were consequently unbothered when over the course of the scheme they learned for a fact that proceeds from narcotics trafficking and hacking crimes were transferred through Samourai. For that reason, the defendants are wrong to suggest in their sentencing submissions that their crimes are akin to a licensing issue or a failure to implement adequate compliance processes. (Rodriguez Letter at 1-2, 6-7; Hill Letter at 2-3; Hill Subm. at 34-35).[2] The defendants' crimes are not predicated on a regulatory lapse, but on the defendants' unambiguous desire, intent, and actions taken to help criminals engage in money laundering and sanctions evasion through Samourai.

For the reasons further discussed below, the Government respectfully submits that a sentence of 60 months' imprisonment for each of Rodriguez and Hill is necessary to satisfy the purposes of sentencing set forth in 18 U.S.C. § 3553(a).

[2] The Rodriguez Letter begins at Dkt. 154-1 at 2. The Hill Submission begins at Dkt. 155 at 1.

II. BACKGROUND

A. Offense Conduct

1. Overview

Between 2015 and April 2024, Rodriguez and Hill developed, marketed, controlled, and operated Samourai, a cryptocurrency mixing service that transferred Bitcoin ("BTC") on behalf of the public in exchange for substantial fees. The purpose of the cryptocurrency mixing service was to make cryptocurrency untraceable, *i.e.*, to conceal its source and owner by obfuscating transactions in BTC that would otherwise be publicly traceable through the blockchain. During this period, Rodriguez served as Co-Founder and Chief Executive Officer of Samourai, while Hill served as Co-Founder and Chief Technology Officer for Samourai. (PSR ¶¶ 9-10).[3] Although Samourai was offered as a "privacy" service to customers, Rodriguez and Hill also knew and intended that Samourai would be a haven for criminals to engage in large-scale money laundering and sanctions evasion. Through Samourai, Rodriguez and Hill earned millions of dollars in fees by laundering the proceeds of drug trafficking, darknet marketplaces (including multiple murder-for-hire solicitations and the distribution of child sexual abuse materials), cyber intrusions and frauds, sanctions evasion, and other criminal activities. Law enforcement has identified at least $237 million of criminal proceeds laundered using Samourai before April 2024, when law enforcement shut down Samourai's servers and arrested Rodriguez and Hill. (PSR ¶ 8). Because Samourai's users often took other, sophisticated steps to conceal the source of their cryptocurrency

[3] Because the offense conduct description and guidelines calculation in the Presentence Reports for Rodriguez and Hill are identical, all citations to the description of the offense conduct and the guidelines calculation are from the Presentence Report for Rodriguez. Citations to Rodriguez's and Hill's Presentence Reports are otherwise cited as "PSR-R" and "PSR-H", respectively.

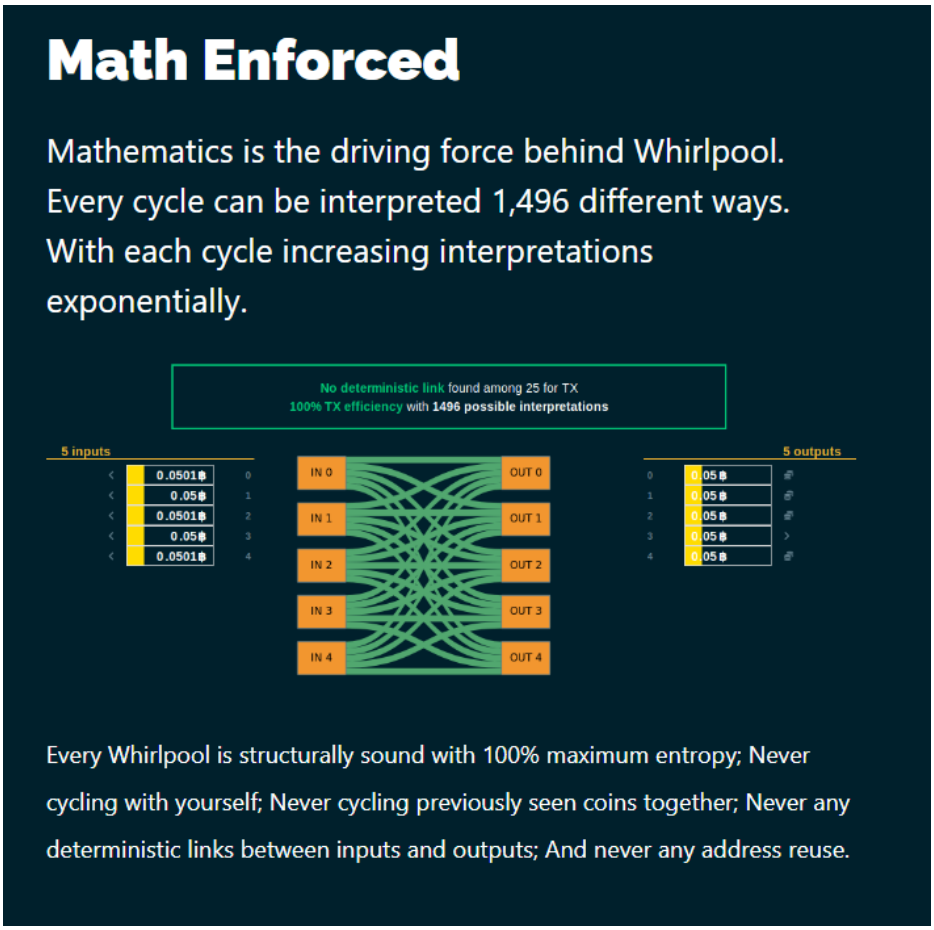
before sending their cryptocurrency to Samourai, it is impossible to track all of the criminal proceeds that were laundered using Samourai and thus this $237 million figure likely understates the volume of crime proceeds that flowed through the platform.

2. Samourai's Operations

Rodriguez and Hill developed Samourai's mobile application, which could be downloaded from the Google Play Store onto a user's cellphone and was downloaded over 100,000 times. After users downloaded the Samourai app, they could store their private keys for any BTC addresses they controlled within the Samourai program. These private keys, however, were not shared with Samourai personnel or Samourai's servers; normally, access to the private key is necessary to transfer Bitcoin from one location on the Blockchain to another. Rodriguez and Hill developed technology that enabled Samourai to execute transfers of its users' BTC from one location on the Blockchain to another, even without possessing the private keys for their users' BTC. To execute and facilitate these transfers, Samourai used a centralized coordinator server (the "Coordinator Server") that was managed and controlled by Rodriguez and Hill. Rodriguez and Hill controlled Samourai's operations and paid its operating expenses—including web hosting services and fees to the Google Play Store—to make Samourai available to users around the world, including in the United States and the Southern District of New York. Rodriguez and Hill advertised the anonymity of Samourai to potential users and thus, by extension, designed Samourai so as to avoid collecting any identifying information, such as email addresses, identification, or names, from its users. (PSR ¶¶ 15, 17).

Rodriguez and Hill instituted two features that were specifically intended to conceal the source of users' BTC. First, Rodriguez and Hill developed a BTC mixing service known as

"Whirlpool," which mixed batches of BTC between groups of Samourai users to prevent tracing of BTC transactions on the Blockchain.[4] (PSR ¶ 16). Samourai's website bragged that it was virtually impossible to link inputs and outputs in even a single Whirlpool transaction, as depicted below:



Second, Rodriguez and Hill developed a Bitcoin transmission service known as "Ricochet," which created additional and unnecessary intermediate transactions (known as "hops") when a user sent Bitcoin from one address on the Blockchain to another. These intermediate

[4] A detailed description of how Samourai's Whirlpool feature functioned is in the PSR at paragraphs 22-23.

transactions served as a layering technique for Samourai users to make it even more difficult to determine that a particular batch of cryptocurrency had actually originated from criminal activity through tracing alone.[5] The Samourai Website bragged that its Ricochet feature could assist customers in further obfuscating the link between customers' deposits and withdrawals, describing the Ricochet feature as a "premium tool that adds extra hops of history to your transaction" and which would allow customers to "[s]tump the blacklists and help guard against unjust 3rd party account closures."[6] (PSR ¶¶ 16, 24).

From the start of the Whirlpool service in 2019 and the Ricochet service in 2017, at least 90,000 BTC (worth over $2.3 billion when applying the BTC-USD conversion rates at the time of each transaction) passed through these two services. Samourai collected fees for both services, totaling at least $5 million in BTC for Whirlpool transactions and at least $1.3 million in BTC for Ricochet transactions, valued at the time the transactions were conducted and the fees collected. (PSR ¶ 16). Given the significant appreciation of Bitcoin, the approximately 246.3 BTC comprising the collective $6.3 million in fees is valued today at over $26.9 million.[7] Between 2015 and 2021, Rodriguez and Hill did not file any U.S. tax returns, and thus did not report any of

---

[5] A detailed description of how Samourai's Ricochet feature functioned is in the PSR at paragraphs 24-25.

[6] "Blacklists" are lists of cryptocurrency addresses known to be associated with sanctioned entities and known criminal activity frequently used by cryptocurrency exchanges to block particular transactions from occurring. For example, the United States Treasury Department's Office of Foreign Assets Control maintains lists of cryptocurrency addresses known to be linked to criminal activities or other threats to the national security, foreign policy, or economy of the United States.

[7] The Government does not have meaningful visibility into how, if at all, the defendants spent their crime proceeds, *i.e.*, the approximately 246.3 BTC in fees they earned.

their income from Samourai. Similarly, Samourai's revenues were not reported during this timeframe on any tax returns associated with corporate entities that were publicly affiliated with Samourai.

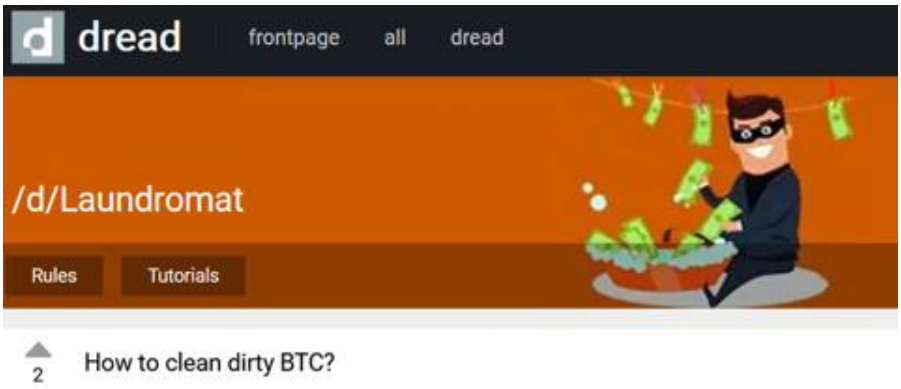
3. Rodriguez and Hill Intended that Criminals Use Samourai to Commit Money Laundering

Rodriguez and Hill intended for criminals to use Samourai to engage in money laundering, and Rodriguez and Hill openly and proactively encouraged and solicited criminals—including hackers, darknet marketplace users, and sanctions evaders—to engage in money laundering transactions using Samourai Wallet. As they admitted during their plea allocutions and as stipulated in their plea agreements, Rodriguez and Hill knew that criminals were in fact using Samourai to launder computer hacking and drug trafficking crime proceeds. (PSR ¶ 26). Indeed, both defendants stipulated in their plea agreements that they "knew or believed that" at least some "of the laundered funds were the proceeds of, or were intended to promote, an offense involving the manufacture, importation, or distribution of a controlled substance." Plea Agreement at 2. Rodriguez and Hill were not merely passive observers—they wanted and intended for criminals to use Samourai to launder crime proceeds, and advertised Samourai accordingly. In their external communications with, and solicitations of, customers, and in their internal communications with other Samourai personnel, Rodriguez and Hill undisputedly expressed their desire that Samourai be used, at least in part, for money laundering.[8]

[8] It should be noted that the set of communications reviewed by law enforcement is just a partial set. Samourai's RocketChat server (a communications platform, akin to Slack) contained encrypted messages, and Rodriguez and Hill configured this server to auto-delete messages older than 30 days. As a result, the Government was able to retrieve few messages from the server, and the majority of what was retrieved was encrypted and inaccessible. The defendants appear to have used RocketChat for particularly important communications. For example, shortly after Hill

For example, on January 5, 2018, in a WhatsApp chat, when asked by an associate what "mixing" was—*i.e.*, what Samourai did and advertised itself as doing—Rodriguez described Samourai as "money laundering for bitcoin." Rodriguez's associate then responded with an emoji expressing fear and surprise: "😳." (PSR ¶ 27(a)).

Similarly, on Dread, a Reddit-like dark web message board featuring discussions about darknet marketplaces, Hill expressly advertised Samourai as a money laundering service to other users. For example, Hill brought up Samourai in a Dread subforum (pictured below) titled "Laundromat," which bore the banner image of a masked criminal washing money in a bathtub (*i.e.*, laundering or cleaning his dirty money), and contained within it a post titled "How to clean dirty BTC":



In this forum, a Dread user asked what were the most "[s]ecure methods to clean dirty BTC" so that the BTC would become "untraceable, clean" and the Dread user would "never get caught." On October 2, 2023, Hill responded by criticizing a competitor mixer ("Mixer-1") and directing

---

learned that he was under investigation following a court order directing that Samourai's servers be copied and taken down, an associate messaged Hill that they were "deploying an emergency rocketchat" to use for future communications.

the Dread user to "Avoid [Mixer-1] at all costs," then encouraged the Dread user to use Samourai, writing that "Samourai Whirlpool is a much better option" to clean dirty BTC.

In another Dread post, Hill again encouraged darknet marketplace customers to use Samourai to conceal their crimes. In a Dread discussion thread in the subforum "DarkNetMarkets," titled "Payments on darknet markets," a Dread user asked why darknet marketplaces still allowed BTC for transactions when "Bitcoin is a well know[n] traceable tool, LE [*i.e.*, law enforcement] have proved it time and time again," and expressed concern that "people [] buying drugs here [are] playing with their freedom." (PSR ¶ 27(b)-(c)). On November 14, 2020, Hill responded by criticizing Mixer-1 and directing the Dread user to "avoid[]" Mixer-1 "at all costs," and then encouraged the Dread user to use Samourai Whirlpool. (PSR ¶ 27(c)).

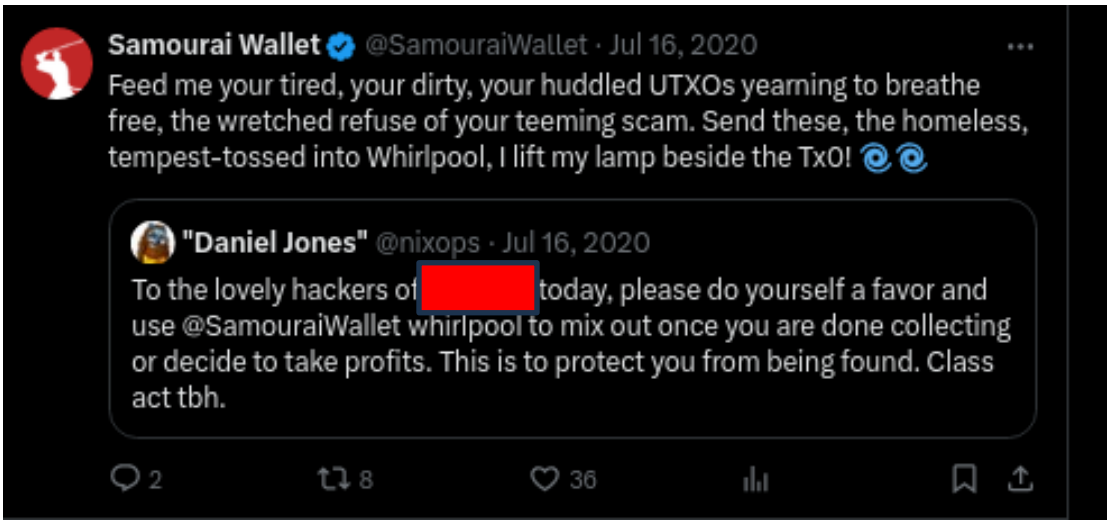
Rodriguez similarly knew that Hill was advertising Samourai to darknet marketplace users. For example, on August 18, 2020, Rodriguez stated in a Telegram thread with an associate: "we're making a space on the dark net boards, dread in particular" and Hill "has been doin[g] a lot of work there." (PSR ¶ 28). Further, in a tweet on February 10, 2022, Hill criticized Samourai's competitor, Mixer-1, for inadequately concealing the crime proceeds from a theft from a cryptocurrency exchange in 2016. Hill reposted an image tracing the crime proceeds from the theft into Mixer-1 and wrote that users should "never use" Mixer-1 to do Samourai's "job"—namely, concealing crime proceeds. (PSR ¶ 31(b)).

Rodriguez similarly made clear in his private communications that he intended for criminals to use Samourai to conceal their crime proceeds, particularly in communications where he criticized Samourai's primary competitor, Mixer-1, for inadequately concealing crime proceeds and risking customers' apprehension by law enforcement. For example, on July 27, 2019, in

private Telegram messages, Rodriguez wrote that Mixer-1 was "playing fast and loose" with its concealment methodology, and "is likely to get someone locked up." Rodriguez's associate replied, "[e]specially as some of the people that have BTC from obvious hacks etc haven't mixed them in a sophisticated way." Rodriguez responded, "yeah it is crazy." (PSR ¶ 28).

In addition, in July 2020, Rodriguez and Hill publicly and privately expressed their desire for criminals to use Samourai in connection with their tracking, in real time, the flow of crime proceeds of a well-publicized hack of a prominent social media company ("Social Media Company-1"). (PSR ¶ 29). In the course of those discussions, the defendants made the following specific statements:

- In a July 16, 2020 tweet (depicted below), after a third party encouraged the "lovely hackers of [Social Media Company-1]" to "use @SamouraiWallet whirlpool to mix out once you are done collecting or decide to take profits" in order to "protect you from being found," Rodriguez responded by personally encouraging the Social Media Company-1 hackers to "[f]eed" and "[s]end" the crime proceeds into "Whirlpool." (PSR ¶ 29(a)).

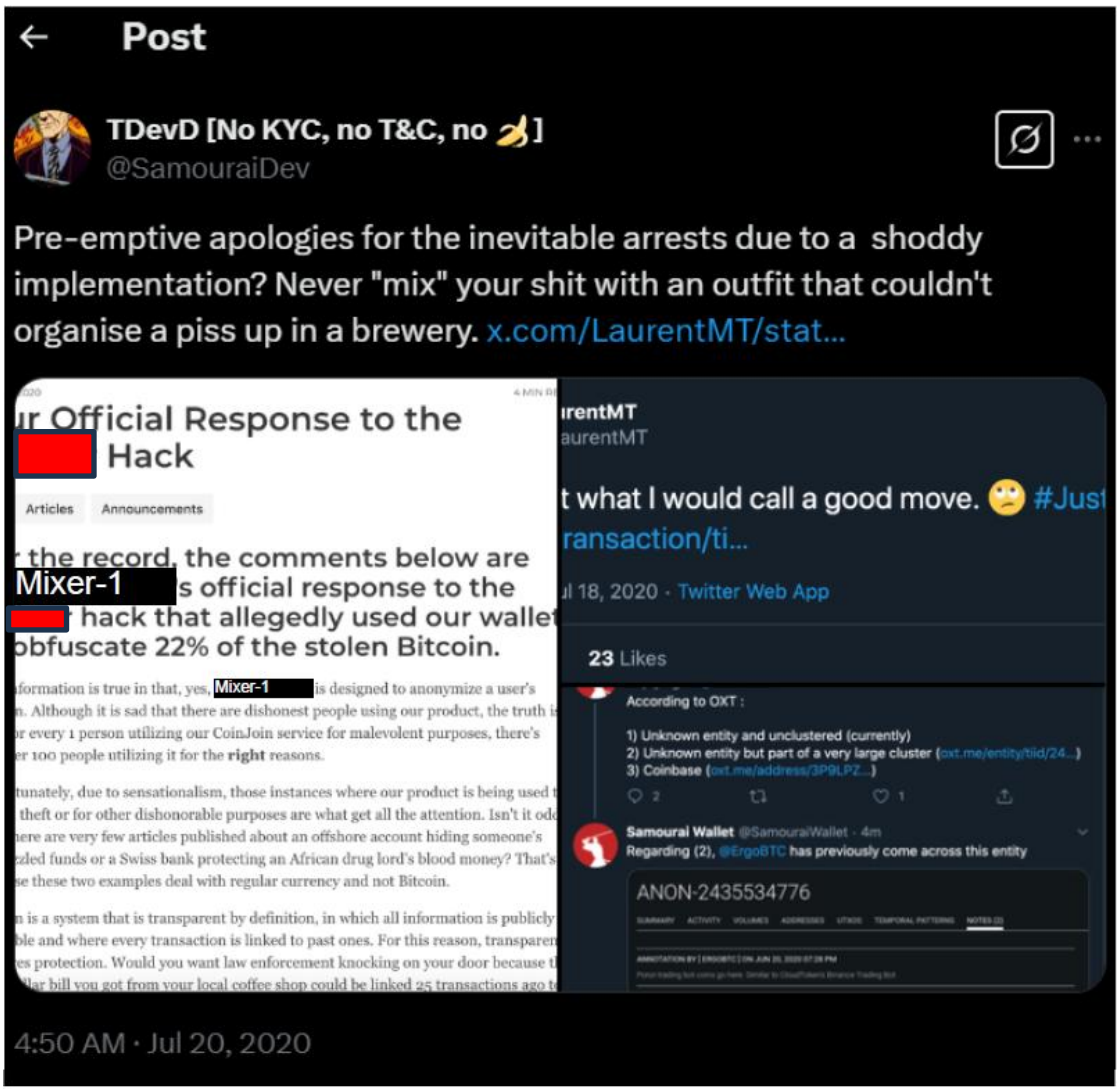


- Later that same day, Rodriguez explicitly referenced the Social Media Company-1 hack in yet another tweet (also depicted below) and offered a promotion to solicit and encourage other hackers to launder crime proceeds through Samourai: "20% OFF all Whirlpool" fees. (PSR ¶ 29(b)).

- The next day, on July 17, 2020, in private Telegram messages, an associate complained about the hackers of Social Media Company-1 using Mixer-1 and not Samourai, writing, "the hackers will get caught – 100%" and musing, "why oh why can't someone high profile use Whirlpool?! I know it isn't necessary but that wou[l]d be so cool." Rodriguez responded, "We were aware of them entering [Mixer-1] 6 hours ago . . . trust me, we're all disappointed." (PSR ¶ 29(c)).

- In the ensuing days, Rodriguez and the associate continued to monitor the movement of the Social Media Company-1 hack crime proceeds on the Blockchain. Three days later, on July 20, 2020, Rodriguez observed that the hackers, in using Mixer-1 and not Samourai to conceal their crime, "are behaving like they want to be caught." (PSR ¶ 29(c)).

- In response to a public statement by Mixer-1 expressing remorse that the Social Media Company-1 hackers used Mixer-1 to launder crime proceeds ("it is sad that there are dishonest people using our product"; "instances where our product is being used to hide a theft"), in a July 20, 2020 tweet (depicted below), Hill criticized Mixer-1 both for its apology and for its inadequate concealment of the crime proceeds, which he predicted would lead to "inevitable arrests."



Hill posted this critique from his Samourai Twitter account with the username "Samourai Dev", thereby advertising Samourai as a service better able to conceal crime proceeds and prevent detection by law enforcement. (PSR ¶ 29(d)).

Notably, Rodriguez and Hill were marketing Samourai to criminal darknet users, and not mainstream cryptocurrency users, knowing that Samourai's features were particularly attractive to those laundering illicit funds. For example, on the Samourai website, Hill and Rodriguez described and advertised Samourai as a "bitcoin wallet for the streets," which was a term Rodriguez had employed before when referring to criminal darknet markets. (PSR ¶ 33) ("If you want a virtual

version of the streets, I mean, shit, it's the dark net markets. Right? What, how more, what, how much more street can you get?"). Similarly, on August 27, 2020, in a private message with another Twitter user (the "Twitter User"), Hill—using the "Samourai Dev" Twitter account—discussed the use of Samourai by criminals operating in online black markets such as Silk Road (emphasis added):

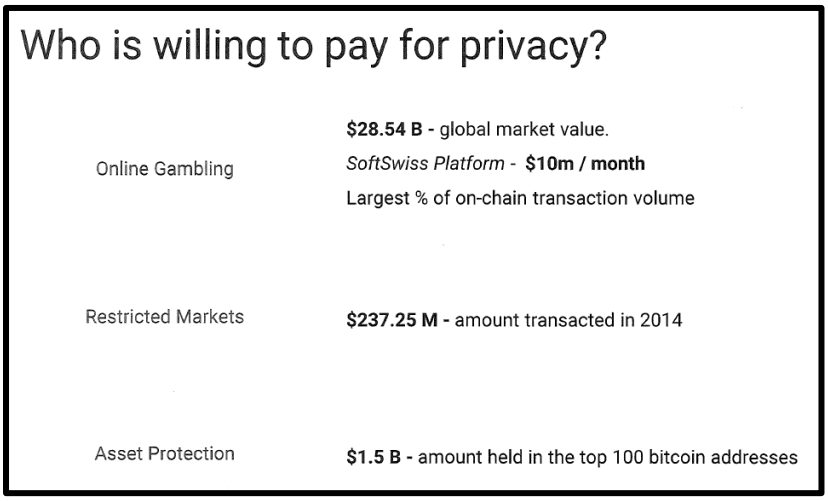
Twitter User: Silk Road is why I first found Bitcoin and the desire to keep engaging in those types of markets is one reason that I want to defend/strengthen those use cases . . .

Samourai Dev: No, not at all. We probably have different views on some basic tenets of bitcoin, you and I – so to each his own so to speak. At Samourai we are entirely focused on the censorship resistance and black/grey circular economy. This implies no foreseeable mass adoption, although black/grey markets have already started to expand during covid and will continue to do so post-covid. . . .

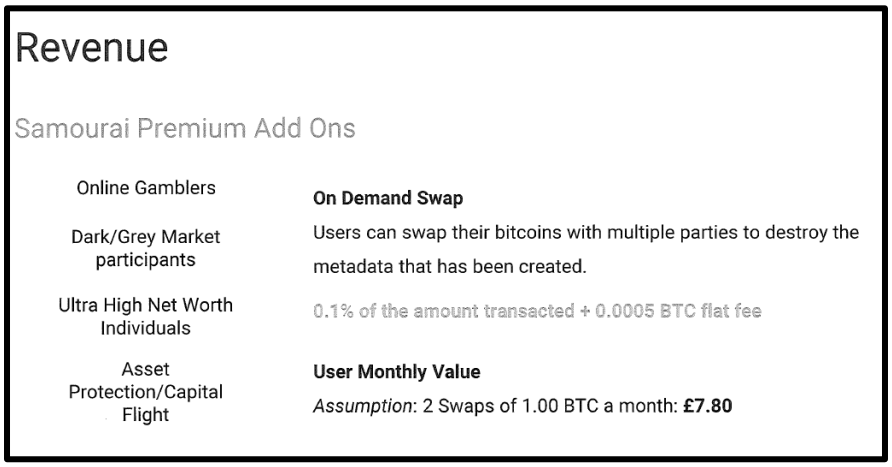
(PSR ¶ 32). Like Hill, Rodriguez knew Bitcoin's primary use was in darknet markets: in tweets posted on November 24, 2019, Rodriguez referred to Bitcoin as "black market money." (PSR ¶ 33). Further, in a Skype conversation where Hill attempted to recruit a software engineer to assist with Samourai, Hill similarly referred to Samourai's work as "on the black," giving the software engineer the option not to participate: "If you are interested, no problem, we can discuss it further. On the other hand, since it is 'on the black' as they say… it's up to you to tell us." (*Id.*).

Rodriguez and Hill also generated and transmitted to potential investors marketing materials, such as those excerpted below, that discussed how Samourai's customer base was intended to include criminals seeking to conceal their crime proceeds and to subvert safeguards and reporting requirements by financial institutions. Marketing materials from Samourai Wallet's email account make clear that, from inception, Samourai was designed with the specific intent that

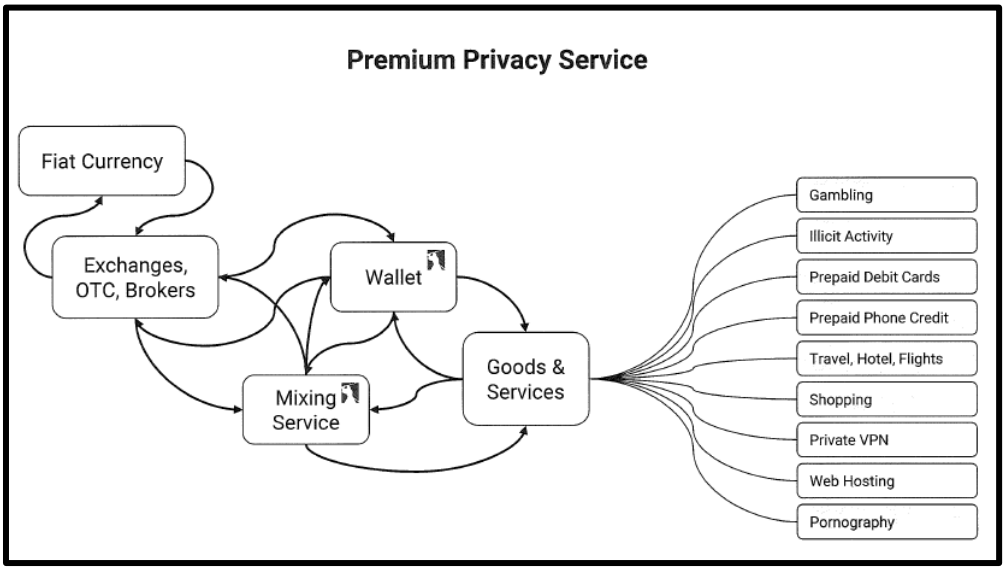
its revenue sources would include criminals laundering crime proceeds. As shown in the marketing slide below, in the description of "who is willing to pay" and anticipated sources of "revenue" for Samourai, the defendants specifically cited "Illicit Activity," "Restricted Markets," and "Dark/Grey Market Participants" as part of Samourai's intended customer base and revenue stream. (PSR ¶ 35).



In the below excerpt from Samourai's marketing materials, Rodriguez and Hill acknowledged that its revenues would be derived from "Dark/Grey Market participants" seeking to "swap their bitcoins with multiple parties" to avoid law enforcement detection. (PSR ¶ 36).

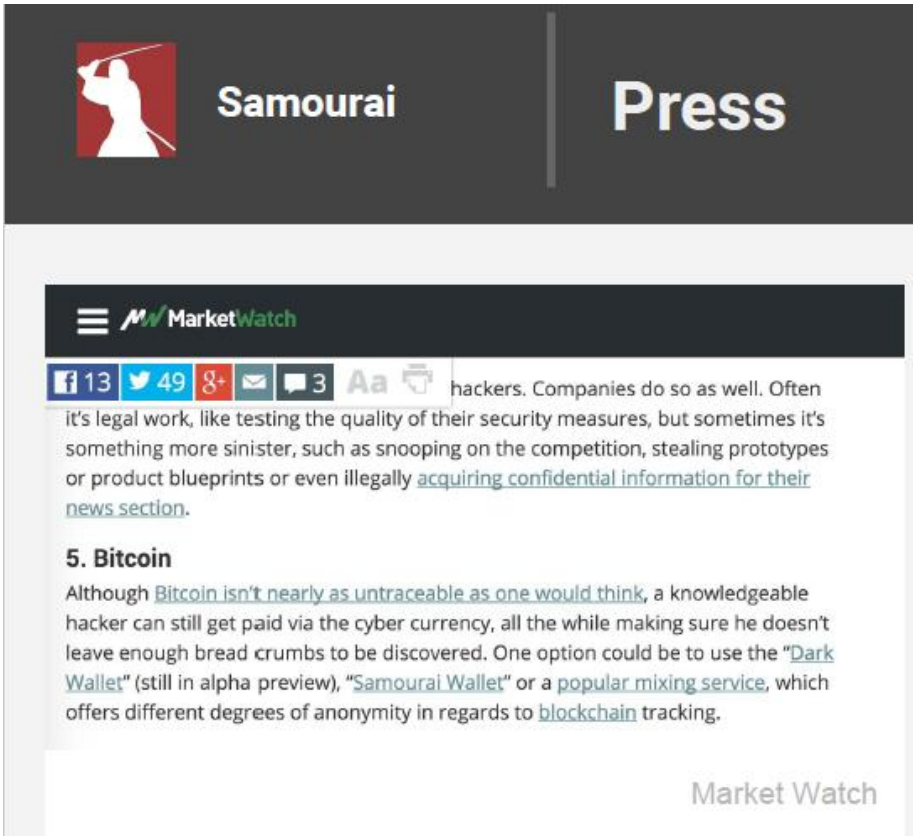


In yet another marketing slide, Rodriguez and Hill promoted Samourai's Wallet and "Mixing Service" as a "Premium Privacy Service" for transactions involving the proceeds of goods and services that included, among other things, "Illicit Activity." (PSR ¶¶ 35-36).



Rodriguez and Hill even incorporated into Samourai's promotional materials third-party reporting identifying Samourai as a money laundering tool. Specifically, on September 1, 2015, Rodriguez emailed Hill with the subject "LOL," and included in the body a link to a press report from August 25, 2015 titled "6 'services' that make hackers rich," which specifically referenced Samourai Wallet. The article noted that "much" of hackers' work "is usually illegal," and further stated that "a knowledgeable hacker can still get paid via [Bitcoin], all the while making sure he doesn't leave enough bread crumbs to be discovered. One option could be to use . . . 'Samourai Wallet' or a popular mixing service, which offers different degrees of anonymity in regards to blockchain tracking." (PSR ¶ 40). On his laptop, Rodriguez excerpted this language from the

press report and included it in Samourai's marketing material, specifically in a PowerPoint presentation dated October 15, 2015. (PSR ¶ 41(b)).[9]

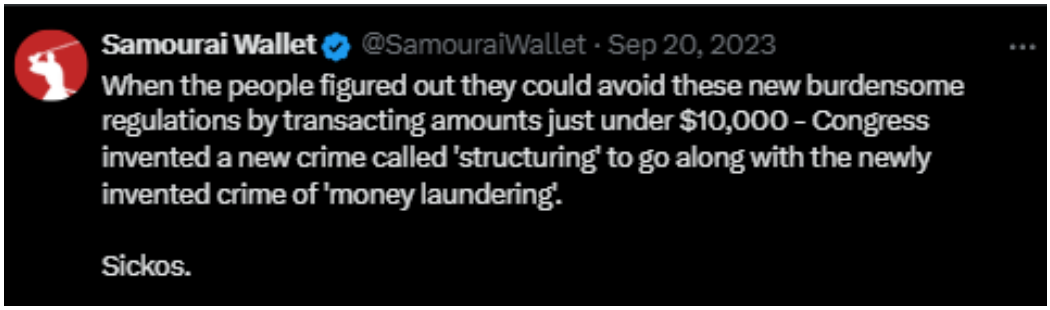


4. Rodriguez and Hill Expressed Disdain for AML and Sanctions Laws

Rodriguez not only solicited criminals to conduct money laundering using Samourai but expressed disdain for laws designed to combat money laundering. Specifically, on September 20, 2023, in response to a third party's tweet criticizing legal reporting requirements triggered when a cash transaction exceeds $10,000, Rodriguez criticized Congress's criminalization of individuals'

[9] Indeed, in his sentencing submission to the Court, Hill's own retained expert, David Yermack, favorably cites to and describes this presentation as an "Investor presentation." (Dkt. 155 at 83, 84 n.5, 87 (citing "USAO_WH_00000024," *i.e.*, this presentation, as a "2015 Samourai investor presentation")).

efforts to evade these reporting requirements: "Congress invented a new crime called 'structuring' to go along with the newly invented crime of 'money laundering.' Sickos." (PSR ¶ 30).



Indeed, Hill expressed no concern when Samourai was identified by law enforcement as a prime money laundering tool. In response to Europol highlighting Samourai as a "top threat" because of its widespread use by criminals to engage in money laundering, Hill posted a message on Twitter on March 16, 2021 (depicted below) suggesting that Samourai had no intention of changing its practices, writing, "Europol also highlighted Samourai Wallet as an emerging 'top threat' in same article. Do you see us shitting in our pants ?" (PSR ¶ 34).

They not only disparaged anti-money laundering laws, Rodriguez and Hill also used Samourai social media accounts to encourage users to evade U.S. and international sanctions using Samourai For example, in a June 30, 2022 tweet (depicted below), in response to a third party tweet observing that "Russian oligarchs use crypto to circumvent EU and international sanctions,"

Rodriguez solicited Russian sanctions evaders to become Samourai users, writing, "Welcome new Russian oligarch Samourai Wallet users." (PSR ¶ 31(c)).

Similarly, in a December 12, 2020 tweet, Rodriguez solicited Iranian sanctions evaders to use Samourai, writing, "Users in Iran should run their BTC acquired via Iranian exchanges in Whirlpool." Rodriguez likewise celebrated Iranian sanctions evaders: in a tweet posted on September 1, 2019 (depicted below), Rodriguez confirmed that Iran was the second largest country by Samourai Wallet downloads after the United States. (PSR ¶ 31(a)).

5. Samourai Was In Fact Used for Money Laundering

Rodriguez and Hill's persistent attempts to solicit criminals to use Samourai for money laundering were successful. At a minimum, at least $237 million in criminal proceeds were laundered through the Samourai Whirlpool and Ricochet services between its launch in 2015 and December 2023. (PSR ¶ 37). The over $237 million dollars of crime proceeds laundered through Samourai came from various criminal sources, as described below. (PSR ¶ 41).

a. **Silk Road Darknet Market**. The Silk Road darknet market ("Silk Road") was a well-known online black market that was in operation from approximately 2011 until 2013 and was used by numerous drug dealers and other criminals to distribute illegal drugs and other illicit goods and services. From at least May 2021 up to and including April 2024, over 3,400 BTC of crime proceeds from a former Silk Road vendor that sold illegal narcotics was laundered through a combination of Samourai's Whirlpool and Ricochet services, worth approximately $144 million at the time of the laundering transactions. (PSR ¶ 41(a)).

b. **Hydra Darknet Market**. The Hydra Darknet Market ("Hydra") was a Russian-language darknet market launched in 2015 that enabled users to buy and sell illegal drugs, fraudulent documents, stolen financial information, and money laundering and mixing services. In 2021, Hydra accounted for an estimated 80% of all darknet market-related cryptocurrency transactions, and since 2015, the marketplace received approximately $5.2 billion in cryptocurrency. In October 2020, approximately 40 BTC of crime proceeds from three Hydra vendors that sold illegal narcotics, worth approximately $440,000 at the time, was laundered through Ricochet. An additional approximately 179 BTC of crime proceeds from other Hydra

vendors, worth approximately $3.8 million at the time, was laundered through Whirlpool. (PSR ¶ 41(b)).

c. **Other Darknet Markets.** Whirlpool was used to launder approximately 213 BTC in crime proceeds, worth approximately $3.9 million at the time of the transactions, from Nucleus Marketplace, Matanga Market, and Kraken, three prominent darknet marketplaces that primarily sold illegal drugs, stolen credit cards, and other illegal merchandise. (PSR ¶ 41(c)).

d. **October 2021 Hack and Spear Phishing Scheme.** In October 2021, a spear phishing scheme compromised the servers of a cloud-service provider and the virtual private server accounts of corporate clients of the cloud-service provider. As a result, between November 2021 and August 2022, approximately 89 BTC of criminal proceeds from the scheme, which was worth approximately $3.7 million at the time, was laundered through Whirlpool. (PSR ¶ 41(i)).

e. **December 2021 Hack.** In December 2021, a decentralized financial platform was hacked, and between June 2022 and November 2023, approximately 2,000 BTC of criminal proceeds, which was worth approximately $51 million at the time, was laundered through Whirlpool. (PSR ¶ 41(g)).

f. **February 2022 Hack.** In February 2022, a web server was hacked and, among other things, a customer database was exfiltrated and cryptocurrency was stolen. As a result, between February and May 2022, approximately 70 BTC of the criminal proceeds, which was worth approximately $2.9 million at the time, was laundered through Whirlpool. (PSR ¶ 41(h)).

g. **July 2022 Hack.** In July 2022, a decentralized financial protocol was hacked, and between January 2023 and March 2023, approximately 54 BTC of criminal proceeds, which was worth approximately $1.4 million at the time, were laundered through Whirlpool. (PSR ¶ 41(e)).

The victim impact of this hack is described in greater detail below in the discussion of the Section 3553(a) factors.

h. **November 2022 Hack.** In November 2022, a cryptocurrency exchange was hacked, and between June 2023 and January 2024 approximately 389 BTC of criminal proceeds, which was worth approximately $13.7 million at the time, was laundered through Whirlpool. (PSR ¶ 41(f)).

i. **February 2024 Hack.** In February 2024, a decentralized cryptocurrency exchange was hacked, and in that same month, approximately 186 BTC of criminal proceeds, which was worth approximately $9.6 million at the time, was laundered through Whirlpool. (PSR ¶ 41(d)).

j. **Other Dark Web Schemes.** In addition to hackers and drug traffickers operating on darknet marketplaces, other types of criminals who typically operate on the dark web used Samourai to launder their crime proceeds and to conceal payments used in the commission of crimes on the dark web. For example, a website on the dark web that distributed child sexual abuse material ("CSAM") solicited Bitcoin payments from users to fund the website's distribution of CSAM material. Between September 2020 and February 2022, an operator of the CSAM website laundered some of those funds using Whirlpool. As another example, in February 2021 and between April and July 2021, two individuals each seeking to hire hitmen through the dark web for two separate murder-for-hire schemes sent the payments to the assassins using Whirlpool. (PSR ¶ 41(j)).

k. **Sanctioned Jurisdictions.** Samourai also laundered funds from sanctioned jurisdictions, such as Iran, Russia, and North Korea, frustrating the Government's carefully-constructed sanctions regimes and national security and foreign policy considerations. For

example, Samourai's Whirlpool system laundered Bitcoin worth over $1.4 million at the time originating from: Nobitex, an Iranian cryptocurrency exchange; Garantex, a Russian cryptocurrency exchange; and Lazarus Group, a hacking group operated by the North Korean Government. (PSR ¶ 41(k)).

6. Rodriguez and Hill Knew That Users Were Actually Laundering Money Through Samourai

There is no question that Rodriguez and Hill had contemporaneous knowledge that their marketing of Samourai in fact resulted in the actual laundering of criminal proceeds. As discussed above, both defendants stipulated in their plea agreements that they "knew or believed that" at least some "of the laundered funds were the proceeds of, or were intended to promote, an offense involving the manufacture, importation, or distribution of a controlled substance." (Plea Agreement at 2). Not only is this obvious given their consistent solicitation of, and marketing to, criminals, but, as part of their operation of Samourai, the defendants actively monitored flows of BTC into Samourai. In particular, the defendants admitted in text messages that they spot-checked large transactions involving Samourai. To conduct their monitoring, Rodriguez and Hill acquired and used, among other tools, the website OXT.me, a free, publicly available blockchain explorer tool that allowed users to trace transactions on the blockchain, and provided attribution for various addresses, such as showing that a particular wallet address was known to be used by a particular hacker, or that a cluster of addresses were attributable to known darknet marketplaces like Silk Road or Hydra Market. (PSR ¶ 38).

In February 2024, three days after a well-publicized, $26 million hack of a decentralized cryptocurrency exchange ("Crypto Exchange-1"), in private Telegram messages, Hill and an

associate discussed how proceeds from computer hacking were flowing through Samourai. On February 19, 2024, Hill and the associate had the following discussion:

Hill: Not sure if you are using 0.5 pool right now but liquidity in that pool is very high as of 72 hours ago

Associate: [Crypto Exchange-1] hacker sent a lot of funds in your pool, they constantly remixing

That's why

Hill: anyway, I'll keep and I [*i.e.*, 'an eye'] on it. Thanks for reaching out

(PSR ¶ 39).

Rodriguez was similarly on notice that Samourai was in fact being used to launder money. For example, Rodriguez had saved to his laptop a January 2019 Drug Enforcement Administration ("DEA") document, marked "law enforcement sensitive," and titled, "Samourai Wallet and Evolving Blockchain Anonymization Methods," which described the likely use of Samourai Wallet by drug trafficking organizations selling drugs in dark web marketplaces. This DEA document identified an increase in users on "dark web forums" discussing how to "defeat blockchain analysis tools." The document further noted that "[t]he use of these tools by law enforcement has become common knowledge following successful actions against dark web drug trafficking organizations (DTOs) in 2017 and 2018" and that users are thus "gravitating towards Samourai Wallet." The DEA document stated that Samourai "has the potential to create significant hurdles for law enforcement cryptocurrency investigations" and will help to "allow advanced dark web users . . . to hide the illegal origins of bitcoin." The document explained that "expert targets"—which include "[d]ark web drug vendors and site administrators"—"are likely already using parts of Samourai's feature-set in one capacity or another." (PSR ¶ 41(c)). Rodriguez also

possessed outside reporting explaining why cryptocurrency mixers like Samourai are popular vehicles for money laundering. Specifically, Rodriguez possessed a Financial Action Task Force ("FATF") report titled "Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing," listed the following "red flags," all of which refer to mixing services like that offered by Samourai: (i) use of a service provider that operates a "mixing" service; (ii) "[t]ransactions making use of mixing and tumbling services, suggesting an intent to obscure the flow of illicit funds between known wallet addresses and darknet marketplaces"; (iii) funds associated with "known suspicious sources, including darknet marketplaces, mixing/tumbling services, questionable gambling sites, illegal activities (e.g. ransomware) and/or theft reports"; and (iv) instances when a customer's funds are sourced from "third-party mixing services." (PSR ¶ 41(d)).

Despite knowing full well that that Samourai's Whirlpool and Ricochet services were being used to conceal crime proceeds, Rodriguez and Hill took no steps to prevent or stop money laundering on Samourai. To the contrary, Rodriguez and Hill described Samourai on its website as a group of "privacy activists who have dedicated our lives to creating the software that Silicon Valley will never build, the regulators will never allow, and the VC's [venture capitalists] will never invest in." (PSR ¶ 42).

7. Rodriguez's Public Communications and Escape Plan Shows His Consciousness of Guilt

Rodriguez's criminal intent is further punctuated by his public acknowledging that he risked incarceration for operating Samourai and an extensive escape plan that was found in his home on the date of his arrest. In a February 3, 2016 tweet, Rodriguez expressed his understanding that he could be imprisoned because Samourai was flouting anti-money laundering ("AML") or

know your customer ("KYC") requirements: "We rather sit in a jail cell than comply with KYC/AML requirements for Bitcoin." (PSR ¶ 42).

In addition, law enforcement recovered from Rodriguez's residence a detailed, six-page handwritten plan for Rodriguez to flee the United States if law enforcement shut down Samourai or planned to arrest the defendants. Among other things, Rodriguez's escape plan set forth that: (a) he planned to travel with multiple passports, a minimum of $10,000 cash, a burner phone, an unused SIM card, an encrypted USB drive, and a burner laptop; (b) he planned to destroy evidence of Samourai's operations; (c) he planned to drive from Pennsylvania to Florida, making sure to evade detection by driving "OFF HIGHWAY," staying in "CASH MOTELS," and paying in "CASH ONLY"; (d) from Florida, Rodriguez planned to take a boat to Jamaica ("HIRE BOAT & CAPTAIN TO GO BY SEA") and potentially fly from Jamaica to Cuba or the United Kingdom; (e) he may travel to meet Hill; (f) he would use a United Kingdom passport while fleeing from law enforcement; (g) there were multiple "STASH" houses in Florida and Pennsylvania where he could store burner phones while fleeing law enforcement; and (h) he would use a storage unit registered in someone else's name associated with a "LOCAL, NON FRANCHISE" company, and paying for it "IN CASH." (PSR ¶ 47). In other words, Rodriguez knew full well that he could be the subject of criminal charges for his operation of Samourai, and had planned to undergo detailed steps to avoid facing the consequences of his crimes.

8. Hill's Dark Web Marketplace Directory Shows His Familiarity With Criminal Activities on the Dark Web

In addition to running Samourai, Hill operated a dark web marketplace directory known as "Hades." In a Telegram message to an associate, Hill advertised a darknet market that, in Hill's words, "has painkillers." Hill's dark web market directory included links to a drug supplier selling

cocaine, MDMA, crystal meth, and oxycodone, and to a weapons suppliers selling 3D-printed guns, including automatic rifles. (PSR ¶ 44).

B. Rodriguez and Hill's Indictment, Guilty Plea, and the Guidelines Calculation

On June 24, 2025, a grand jury returned a superseding indictment charging Rodriguez and Hill with participating in a conspiracy to commit money laundering, in violation of 18 U.S.C. § 1956(h) (Count One); and participating in a conspiracy to operate an unlicensed money transmitting business involving the transmission of funds that were known to the defendant to have been derived from a criminal offense or were intended to be used to promote or support unlawful activity, in violation of 18 U.S.C. § 371 (Count Two). On July 30, 2025, Hill and Rodriguez each pleaded guilty to Count Two of the superseding indictment pursuant to separate plea agreements.

Each plea agreement included a stipulation regarding the application of the United States Sentencing Guidelines to the criminal conduct:

1. Pursuant to U.S.S.G. § 2S1.1(a)(2), the base offense level is 8 plus the number of offense levels from the table in § 2B1.1 corresponding to the value of the laundered funds. Pursuant to U.S.S.G. § 2B1.1, 26 levels are added because the value of the laundered funds was more than $150,000,000. Accordingly, the base offense level is 34.

2. Pursuant to U.S.S.G. § 2S1.1(b)(1), a 6-level enhancement applies because § 2S1.1(a)(2) applies, and the defendant knew or believed that any of the laundered funds were the proceeds of, or were intended to promote, an offense involving the manufacture, importation, or distribution of a controlled substance.

3. Pursuant to U.S.S.G. § 4C1.1, a two-level decrease applies because the defendant satisfies all of the criteria set forth therein.

4. Pursuant to U.S.S.G. § 3E1.1(a) and (b), three levels are removed for acceptance of responsibility.

These calculations result in an applicable Guidelines offense level of 35 and a Criminal History Category of I, resulting in a Guidelines range of 168 to 210 months. However, because the

statutory maximum sentence of imprisonment for a violation of Section 371 is 60 months, the applicable Guidelines sentence is 60 months' imprisonment (the "Stipulated Guidelines Sentence"). The PSRs for each respective defendant contain the same Guidelines calculation as that set forth in each corresponding plea agreement. (PSR ¶¶ 52-66, 108). The Probation Office recommends a downward variance sentence of 42 months' imprisonment for each of Rodriguez and Hill. The defendants each request a below-Guidelines sentence; a year and a day for Rodriguez (Rodriguez Subm. at 3),[10] and time served for Hill (Hill Subm. at 32).

III. DISCUSSION

A. Applicable Law

As the Court is aware, the Guidelines still provide important guidance to the Court following *United States v. Booker*, 543 U.S. 220 (2005), and *United States v. Crosby*, 397 F.3d 103 (2d Cir. 2005). Indeed, although *Booker* held that the Guidelines are no longer mandatory, it also held that they remain in place and that district courts must "consult" the Guidelines and "take them into account" when sentencing. *Booker*, 543 U.S. at 264. As the Supreme Court stated, "a district court should begin all sentencing proceedings by correctly calculating the applicable Guidelines range," which "should be the starting point and the initial benchmark." *Gall v. United States*, 552 U.S. 38, 49 (2007).

After that calculation, however, a sentencing judge must consider seven factors outlined in Title 18, United States Code, Section 3553(a): (1) "the nature and circumstances of the offense and the history and characteristics of the defendant"; (2) the four legitimate purposes of sentencing, as set forth below; (3) "the kinds of sentences available"; (4) the Guidelines range itself; (5) any

[10] The Rodriguez Submission is at Dkt. 154.

relevant policy statement by the Sentencing Commission; (6) "the need to avoid unwarranted sentence disparities among defendants"; and (7) "the need to provide restitution to any victims." 18 U.S.C. § 3553(a)(1)-(7); *see also Gall*, 552 U.S. at 50 & n.6.

In determining the appropriate sentence, the statute directs judges to "impose a sentence sufficient, but not greater than necessary, to comply with the purposes" of sentencing, which are:

> (A) to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for the offense;
> (B) to afford adequate deterrence to criminal conduct;
> (C) to protect the public from further crimes of the defendant; and
> (D) to provide the defendant with needed educational or vocational training, medical care, or other correctional treatment in the most effective manner.

18 U.S.C. § 3553(a)(2).

B. <u>A Guidelines Sentence of 60 Months' Imprisonment Is Necessary</u>

The Government respectfully submits that the Stipulated Guidelines Sentence of 60 months would be sufficient, but not greater than necessary, to serve the purposes of sentencing, for Rodriguez and Hill, respectively. This sentence is justified by the gravity and scope of Rodriguez and Hill's crimes, which spanned close to a decade; the need to provide just punishment and achieve general deterrence; and the importance of accounting for the serious criminal activities the defendants supported, encouraged, concealed, and profited from, by intentionally providing money laundering services to criminals.

1. <u>The Nature and Seriousness of the Offense and the Need for Just Punishment</u>

The Stipulated Guidelines Sentence of 60 months' imprisonment is necessary to reflect the nature and circumstances of the offense and to provide just punishment. *See* 18 U.S.C. §§ 3553(a)(1), (2)(A).

The defendants' criminal conduct was serious, extensive, and long running, lasting almost a decade. Through Samourai, the defendants created and operated a popular money laundering tool which both promoted crimes and helped criminals on the dark web and sanctions evaders conceal their crime proceeds. Put simply, Samourai enabled criminality on a vast scale. As a conservative estimate, between Samourai's launch in 2015 and December 2023, criminals laundered BTC worth at least $237 million (valued at the time of the transactions, but worth far more today) in crime proceeds using Samourai's Whirlpool and Ricochet functions. This estimate is conservative precisely because the tools the defendants designed and deployed to conceal the source of BTC that passed through Samourai, including BTC derived from criminal activity, were so effective. [11]

The defendants' money laundering tools were used to further myriad criminal schemes around the world, including complex multi-million-dollar cryptocurrency hacks, international drug trafficking on the dark web, murder-for-hire plots, the distribution of CSAM, and the criminal activities of the North Korean hacker collective Lazarus Group, as well as sanctions evasion.

The defendants engaged in exhaustive planning to create Samourai, dedicating substantial time and energy to its creation, operation, and marketing; indeed, Hill describes Samourai in his

[11] In support of their arguments that Samourai was largely legitimate, Rodriguez and Hill argue that the at least $237 million of traceable crime proceeds was a small fraction of the 90,000 BTC or $2.3 billion (valued at the time of the transactions) that flowed through Whirlpool and Ricochet, and that the remainder otherwise "had no detectable connection to any criminal activity." (Rodriguez Subm. at 8; *see also* Hill Subm. at 28 (claiming "87.5% did not" represent proceeds of crime)). As noted above, because of the complexity and scope of Samourai's operations, the Government has not attempted to trace and has not been able to trace every Bitcoin that entered Whirlpool and Ricochet. The only conclusion the Government can state regarding the balance of the $2.3 billion is that the source of those Bitcoin, whether legitimate or illegitimate, is unknown.

sentencing submissions as his life's work. (Hill Subm. at 38). Those efforts specifically considered Samourai's anticipated criminal use. Samourai was designed to be attractive to criminals by being straightforward and frictionless on the front end, even though the technology was incredibly complex and sophisticated on the back end. And the defendants profited substantially through their operation of Samourai in the manner. The defendants collected over $6.3 million in fees for processing the criminal proceeds law enforcement has been able to identify to date, valued at the time the fees were collected.[12]

Rodriguez and Hill were not mere bystanders to the money laundering conducted through Samourai; they affirmatively wanted criminals to use Samourai to commit money laundering and marketed Samourai accordingly.[13] The defendants' communications—both public and private--and Samourai's marketing materials indisputably show that the defendants intended, from Samourai's inception, to solicit criminals seeking to hide their crime proceeds as at least part of Samourai's customer base.

As detailed above, in 2018, Rodriguez explicitly defined "mixing"—the service Samourai provided—as "money laundering for bitcoin." (PSR ¶ 27(a)). Rodriguez and Hill advertised to and sought out users engaged in serious crimes on darknet market message boards, suggesting that

---

[12] As stated above, given the significant appreciation of Bitcoin, the 246.33385379 BTC comprising the $6.3 million in fees is valued today at over $26.9 million.

[13] While, as Rodriguez points out in his submission, the defendants did not plead guilty to the money laundering conspiracy charged in Count One, (Rodriguez Subm. at 7-8), this Court may consider all facts relevant to the offense, *see* 18 U.S.C. § 3553(a)(1), as well as, "without limitation, any information concerning the background, character and conduct of the defendant," U.S.S.G. § 1B1.4. It is self-evident that this Court may consider the record evidence showing that the defendants actively solicited criminals engaged in money laundering, even if those facts did not lead to a conviction.

Samourai could clean dirty BTC and render it "untraceable." (PSR ¶ 27(b)). By targeting darknet users, the defendants knew precisely the type of criminals they were attracting to the platform, particularly because Hill operated his own directory of darknet markets that included links to a drug supplier and a weapons supplier. On the darknet, in public tweets, and in private Telegram messages, Rodriguez and Hill repeatedly criticized its primary competitor, Mixer-1, on the basis that criminals would get "locked up" by law enforcement if they tried to launder their crime proceeds using Mixer-1, and encouraged criminals instead to use Samourai, which would better conceal their crime proceeds and avoid detection by law enforcement. (PSR ¶¶ 27(b)-(c), 28, 29). The fact that Rodriguez explicitly confided that he and Hill were "disappointed" when high-profile hackers of a social media company used Mixer-1 instead of Samourai to launder their crime proceeds, shows that Rodriguez and Hill wanted and intended for such high-profile hackers (and other criminals) to use Samourai. (PSR ¶ 29(c)).

Moreover, publicly and privately, Rodriguez and Hill stated that Samourai was not primarily targeting "mass adoption," but instead "the streets," "darknet markets," and "black" markets, which plainly refer to criminal marketplaces where contraband is trafficked. (PSR ¶¶ 32, 33). Rodriguez and Hill's marketing slides for Samourai likewise identified "Illicit Activity," "Restricted Markets," and "Dark/Grey Market Participants" as part of Samourai's intended customer base and revenue stream, and their promotional materials—favorably cited by Hill's retained expert—incorporated a press report identifying Samourai as an effective tool for criminal hackers to evade detection. (PSR ¶¶ 34, 35 40, 41(b)). Further, Rodriguez and Hill publicly and actively encouraged sanctions evaders, from jurisdictions such as Iran, Russia, and North Korea, to use Samourai. (PSR ¶¶ 31(a), (c), (d)).

Taken together, the defendants' public and private statements, spanning multiple years, leave no doubt that the defendants, at the outset, wanted criminals to join Samourai and use it to hide their crime proceeds, and were well aware that they did so. In other words, Rodriguez and Hill were not just aware of Samourai's misuse, they designed Samourai, at least in part, to help criminals evade law enforcement detection and frustrate the efforts of victims and law enforcement to locate crime proceeds.

By conspiring to knowingly transmit criminal proceeds and facilitating money laundering, Rodriguez and Hill exacerbated the harm to victims of the criminal schemes enabled by Samourai's operations. Although Rodriguez and Hill had no known role in the underlying hacks, narcotics trafficking, CSAM distribution, or murder-for-hire plots, the money laundering Rodriguez and Hill facilitated played an important role in ensuring the success of the underlying crimes by helping the perpetrators hide their crime proceeds, preventing their recovery by law enforcement and victims, and by concealing the identities of the perpetrators, thus preventing their arrests. Indeed, Rodriguez's and Hill's statements described above, in which they claimed Samourai would do a better job than Mixer-1 at making proceeds of computer hacking untraceable and preventing the hackers' arrest by law enforcement, shows that at least one of the purposes of Samourai was to obstruct law enforcement and prevent financial recovery for victims. In other words, Rodriguez and Hill's offense amplified the victim impact of the underlying crimes.

Those crimes, and the laundering of funds that Samourai enabled, were not mere technical infractions: they had a material impact on real victims. This is compellingly underscored by the victim's statements in connection with *United States v. Ahmed*, a prosecution in this District of a hacker who stole funds from a decentralized cryptocurrency exchange called Nirvana Finance

("Nirvana"). *See United States v. Ahmed*, No. S1 23 Cr. 340 (VM), (S.D.N.Y. Apr. 1, 2024) Dkt. 47 at 13-14, 19-22; Dkt. 47-2 at 1-2; Dkt. 47-3; Dkt. 53. "In July 2022, a decentralized finance protocol [*i.e.*, Nirvana] was hacked, and between January 2023 and March 2023, approximately 54 BTC of the criminal proceeds was laundered through Samourai's Whirlpool, which was worth approximately $1.4 million at the time." (PSR-R ¶ 43.e; PSR-H ¶ 46.e). While the hack itself caused pecuniary harm, the use of Samourai to obscure the hacker's identity exponentially increased the ramifications of this crime. The victim of the Nirvana hack, namely, Nirvana's co-founder, lost most of his life savings as a result of the hack, and described that day as the "worst day of his life." Cieran Lyons, *Nirvana Finance co-founder recounts the 'worst day' of his life*, Cointelegraph, June 2, 2024, https://cointelegraph.com/news/nirvana-finance-founder-hoffman-2022-exploit-shook-his-world.

The laundering exacerbated this tangible harm. As the victim stated, the victim's efforts to uncover the perpetrator of the hack on Nirvana lasted 17 months despite "best efforts from blockchain investigators," which kept hitting "dead ends" due to the sophistication of the hacker's laundering, including through the use of Samourai. *Id.* The hacker's methods were so sophisticated that the victim *never* independently uncovered the hacker's identity: the hacker's crime only came to light because he voluntarily disclosed his conduct to law enforcement. It is thus far from certain that the hacker could *ever* have been caught given his laundering through Samourai. The concealment of the hacker's identity—an anonymity that Samourai afforded its users—resulted in further, serious collateral consequences: because the hacker was unknown, the victim was falsely accused online of having perpetrated the hack himself, and as a result, as the

victim explained in his statement: "I got dozens of death threats and threats to hurt my wife, my mom, and my kids; it was nonstop." *Id.*[14]

In sum, the victim suffered serious and lasting harm because of the difficulty in tracking and holding accountable the true perpetrator of the Nirvana hack. As the victim explained in detail in his victim impact statement:

> In addition to the financial damages to Nirvana's user base, the personal and financial toll on our team has been considerable during this time. The aftermath of the theft saw us grappling with the immediate financial repercussions of losing our livelihoods overnight, coupled with the daunting task of restoring our platform's integrity and user confidence. In addition, in this industry, a team's reputation is extremely important. Until [the hacker's] guilty plea proved we were not responsible, our team endured significant reputational damage.
>
> The strain of these efforts has taken a significant emotional and psychological toll on every member of our team, compounding the financial damage with a profound personal and professional impact.
>
> . . .
>
> The funds stolen and laundered through sophisticated means reflect a blatant disregard for the law and the principles upon which decentralized finance stands.

Ahmed, No. S1 23 Cr. 340 (VM), Dkt. 47-2 at 1-2. The Nirvana hack is just one example of how Samourai's anonymization exacerbated harm to victims of the underlying offenses. It puts the lie to the suggestion that the defendants' conduct was "victimless."

The defendants' criminal conduct also imposed a societal harm. "Title 18 U.S.C. § 1960 was enacted in order to combat the growing use of money transmitting businesses to transfer large

---

[14] Up until the hacker was publicly identified, detailed public speculation by blockchain enthusiasts also falsely pointed to a purported suspect in Brazil, showing the cascading harms of the hack on innocent third parties around the world. *Ahmed*, No. S1 23 Cr. 340 (VM), Dkt. 53 at 8, 15.

amounts of the monetary proceeds of unlawful enterprises." *United States v. Velastegui*, 199 F.3d 590, 593 (2d Cir. 1999). The Sentencing Guideline at issue, 2S1.1, "measures the harm to society" that the illegal movement of crime proceeds "causes to law enforcement's efforts to detect the use and production of ill-gotten gains." *United States v. Allen*, 76 F.3d 1348, 1369 (5th Cir. 1996). "This is so because the harm from such a transaction does not generally fall upon an individual, but falls upon society in general." *United States v. Thompson*, 40 F.3d 48, 51 (3d Cir. 1994) (citation and alteration omitted). "Each unlawful monetary transaction harms society by impeding law enforcement's efforts to track ill-gotten gains." *United States v. Martin*, 320 F.3d 1223, 1227 (11th Cir. 2003). As these authorities have recognized, the defendants' offense conduct imperiled the integrity of the U.S. financial system, causing harm to the public more broadly.

The Government views the defendants as equally culpable. Both Rodriguez and Hill: pleaded guilty to the same offense, participated in the offense for the same span of time, they co-founded Samourai, worked full-time at Samourai during the majority of the charged period as C-suite executives, and effectuated their criminal scheme through multiple, daily acts spanning the entirety of the charged period from 2015 to April 2024. Moreover, their offense level and criminal history computations under the Sentencing Guidelines are identical. While there are differences between them,[15] the Government believes that these differences are approximately equivalent and,

[15] Rodriguez was the Chief Executive Officer and Hill was the Chief Technology Officer, but given their knowledge, cooperation, and leadership, the differences in title are immaterial to their culpability. In addition, although Rodriguez—not Hill—possessed an elaborate escape plan, demonstrating his consciousness of guilt, Hill—not Rodriguez—operated a dark web marketplace directory and was more active, day-to-day, on darknet message boards. Thus these inflection points are, in the Government's view, on substantially equal footing.

on balance, each defendant is equally deserving of the Stipulated Guidelines Sentence of 60 months.

2. The Defendants Minimize the Scope and Gravity of Their Conduct

Although the defendants admitted in their plea allocutions and plea agreements that they knew criminal drug traffickers and hackers used Samourai to conceal their crime proceeds, the defendants, at several points in their sentencing submissions, minimized their offense conduct and downplayed or outright denied their marketing of Samourai to criminals for money laundering.[16] The defendants make various arguments in this vein. They both emphasize that the main goal of Samourai was to enhance privacy on the Blockchain[17] (Rodriguez Subm. at 2, 7; Rodriguez Letter

---

[16] Hill concedes, though undersells, his intent for criminals to use Samourai to launder crime proceeds, admitting that "he took things way too far when he . . . actively encouraged its use for money laundering." (Hill Subm. at 1; *see also* Hill Letter at 3 ("our marketing suggesting that computer hackers and other criminals should use Samourai instead of our main competitor's wallet spiraled well beyond acceptable limits.")

[17] Hill claims that he and Rodriguez created Samourai to frustrate Chainalysis and other forensic companies that conducted sophisticated blockchain tracing and wallet attribution because they were "stripping bitcoin of the privacy and fungibility that were the Cypherpunks' ideals." (Hill Subm. at 24). The Government notes, however, that Hill and Rodriguez operated OXT.me, a free, public blockchain explorer that was also a tool for blockchain tracing and wallet attribution, including for Silk Road and Hydra Market. (PSR ¶ 38). Thus, it appears that Hill's animating concern was not fidelity to anonymity, but hostility to forensic companies--like Chainalysis--known to assist law enforcement.

Likewise, notwithstanding Rodriguez and Hill's strong pro-privacy public comments, they did not always practice what they preached. As confirmed by law enforcement's seizure and analysis of Samourai's servers, despite claiming that Samourai was a "privacy" service, Rodriguez and Hill retained sufficient information to trace or "demix" its mobile users' Whirlpool transactions. In other words, with this information, one could for many Whirpool transactions, with complex analysis, connect the input and output of a Whirpool transaction (although this does not deanonymize the transactions). Rodriguez and Hill collected the information by requiring users to share their extended public key ("XPUB") information with the Coordinator Server. While there was no technical or operational necessity to do so, the defendants chose to retain their mobile users' XPUB information on Samourai's servers. This allowed the defendants to cross-reference

at 6; Hill Subm. at 17, 19). But Rodriguez and Hill's public and private statements and their Samourai marketing materials unmistakably reveal that, even if general user privacy generally was *one of* the overarching features of the platform, soliciting criminals to use Samourai was likewise a feature, and one that the defendants expressly touted.[18]

With respect to Hill, his instant attempts to disavow or downplay his public statements is no more than a transparent bid for leniency at sentencing. Hill—in an about-face from his yearslong public persona—brushes off his prior public and private statements, claiming they were simply "guerilla" marketing and "must be understood in the context of his autism."[19] (Hill Subm. at 36; Hill Letter at 106). Hill's disavowals ring hollow. As explained above, his contemporaneous statements are not ambiguous and self-evidently promoted Samourai as a tool for criminals. Hill's statements were made over a period of years, in multiple public and private forums, and were consistent in tone and content—they demonstrate that Hill meant what he said, and these statements were not merely marketing hyperbole. Indeed the argument that this could have been the purpose of Hill's *private* communications with colleagues and associates strains credulity.

XPUB information with past, present and future Whirlpool transactions to associate input and output addresses belonging to its mobile-only users. After law enforcement seized Samourai's servers, Hill messaged an associate, "Not good," and noted "I'm not thinking so much about Whirlpool as I am about the wallet backends (xpubs)." (PSR ¶¶ 19-20).

[18] Rodriguez and Hill do not dispute the substance of their statements or marketing materials. They only dispute the inferences that can be drawn from them regarding Rodriguez's and Hill's intent to solicit criminals as Samourai users.

[19] Hill also claims that his autism "reduces his moral culpability." (Hill Subm. at 28). The Government acknowledges that the Court should consider Hill's autism as relevant to the "history and characteristics of the defendant," but the defendant has not shown or even attempted to show that his autism precluded him from understanding right from wrong, and the Court should reject any suggestion that the defendant's autism "reduces his moral culpability."

Further, Hill's claim that he "set out to promote the service on darknet markets with the intention of recruiting those who had to move funds for political reasons or to obtain medical remedies that were not reimbursed by their health insurance or lack thereof," (Hill Letter at 3), is wholly unbelievable given the actual (not asserted) context of those particular discussions. As discussed in more detail above, in one such conversation, Hill advertised Samourai in a dark web subforum titled "Laundromat," in a post titled "How to clean dirty BTC," in response to a user asking what were the most "[s]ecure methods to clean dirty BTC" so that the BTC would become "untraceable, clean" and the user would "never get caught."

Needless to say, this is not a forum relating to victims of political persecution or those unable to obtain insurance coverage for needed medical treatments. Nothing in Rodriguez and Hill's communications back up Hill's current claims. To the contrary, Samourai's website, advertisements, and statements on social media make clear that Rodriguez and Hill were aligning themselves with criminals seeking to evade law enforcement detection—actively encouraging and bragging about the money laundering that was taking place on their service.

Separately, the defendants, particularly Rodriguez, also seek to minimize their offense conduct by framing it as a mere failure to obtain a license and implement compliance measures. (Rodriguez Letter at 1, 2, 6; Hill Letter at 2, 3; *see* Hill Subm. at 34). Those arguments mistake the gravamen of this case. The defendants pleaded guilty to conspiring to violate Title 18, United States Code, Section 1960(b)(1)(C), which makes it a crime to operate a money transmitting business where the defendant *knows* the transmitted funds derive from a crime or are to be used to promote a crime. As litigated at length in the defendants' meritless pretrial motions, which this Court denied in full, the offense of conviction has nothing to do with state or federal licensing

requirements, FinCEN regulations, or the Bank Secrecy Act. (Dkt. 118 at 15-19). The defendants' crime was the operation of a business that transmitted Bitcoin knowing that large amounts of that Bitcoin derived from crime. Again, based on the clear record evidence, the defendants not only *knew* criminals were using Samourai to conceal their crime proceeds, but they also *wanted and intended* this use of Samourai by criminals. The defendants' efforts to minimize their conduct as a mere technical licensing or compliance failure at best misapprehends (and at worse misstates) the basis for their criminal convictions. Their persistent and incorrect characterization of their criminal liability fails to appreciate the nature and seriousness of their criminal conduct.

Moreover, although the defendants do not dispute their guilt, they nonetheless seek to minimize their conduct by claiming they relied on counsel to advise them that Samourai's operations were legal. (Rodriguez Letter at 2, 6; Hill Letter at 2). The Court should disregard this argument, other than to view it as an unconvincing and troubling effort to shift blame to their lawyers or the lawyers of third parties.[20]

Lastly, to the extent the defendants imply from their arguments that they sought to operate Samourai as a legal business offering legal services to the public, that is not borne out by the facts. Neither Rodriguez nor Hill paid taxes on their Samourai income; indeed, neither defendant filed any tax returns in the United States from 2015 to 2021. Nor were Samourai's revenues reported

[20] For the avoidance of doubt, the defendants have provided no discovery regarding any advice of counsel defense and have offered no information regarding what the purported advice was, what information was provided by the defendants to solicit the advice, when the advice was provided, or who provided the advice. There is thus no basis on which to evaluate the purported advice of counsel in the context of a mitigation argument. Moreover, based on the context in the sentencing submissions, it appears that the legal advice, to the extent there was any, concerned FinCEN regulations which, no matter how many times the defendants futilely invoke them, simply are not relevant to the crime to which the defendants pleaded guilty.

during this timeframe on any tax returns associated with corporate entities that were publicly affiliated with Samourai. Rodriguez, moreover, had a thorough escape plan to leave the United States and become a fugitive if he were wanted by law enforcement, as described above, thus demonstrating his understanding that he was engaged in criminal conduct by operating Samourai. As to Hill, his solicitation of Samourai users on the darknet while simultaneously operating a darknet directory linking markets unlawfully selling guns and drugs underscores Hill's knowledge that he was encouraging criminals to use Samourai for laundering. In sum, the defendants intended Samourai to be, at least in part, an unlawful business that offered money laundering services for criminals.

3. Specific Deterrence and the Need to Promote Respect for the Law Warrant 60 Months' Imprisonment

Specific deterrence and the need to promote respect for the law also militate in favor of the Stipulated Guidelines Sentence of 60 months' imprisonment. The defendants' actions were far from a one-time mistake or a fleeting lapse in judgment. As noted above, Rodriguez and Hill carried out their crimes for nearly a decade and only stopped when they were arrested. Rodriguez and Hill designed, marketed, and operated Samourai in significant part to facilitate crimes. This was not a one-click, one-time crime. This was their full-time jobs. Again, it required detailed planning, technical expertise, and a willingness to solicit and transmit known crime proceeds, enabling them to collect over $6.3 million in fees. And because the defendants have persistently miscast and minimized their conduct, it is evident that they fail to fully appreciate the seriousness of their conduct, further indicating that specific deterrence is warranted.

The defendants made a knowing decision to pursue a criminal livelihood built on the profits of drug traffickers, CSAM distributors, hackers, and other criminals—and doubled down on that

plan, year after year, thus supporting the criminal users of their business. Their crimes thus appear to have been motivated at least in part by greed and perhaps misguided confidence that they would not get caught. While the Court should of course consider the defendants' personal and familial backgrounds discussed in the sentencing submissions and the Presentence Reports, the defendants' backgrounds do not *ipse dixit* support leniency. At the time of their crimes, the defendants were sophisticated web developers with eminently employable skills and earning potential. There was no financial need or other imperative justifying the defendants' operation of a business that transmitted known crime proceeds. Rather than apply their considerable technical gifts to lawful pursuits, they instead profited handsomely by transmitting known crime proceeds. In short, there was absolutely no need for the defendants to turn to crime. They did so because they wanted to.

The need to promote respect for the law also supports the Stipulated Guidelines Sentence of 60 months' imprisonment. The defendants' offense conduct and private and public statements evince a blatant lack of respect for the law. As previously stated, from inception, Samourai was designed with the specific intent that its revenue sources would include crime proceeds. In the descriptions of "who is willing to pay" and anticipated sources of "revenue" for Samourai in marketing materials maintained by the defendants, they state that they specifically intended that "Illicit Activity," "Restricted Markets," and "Dark/Grey Market Participants" would be part of Samourai's intended customer base and revenue stream. Further, in their own marketing materials, the defendants favorably included a press report that cited Samourai as a service used by illegal

hackers to evade detection.[21] Both Hill and Rodriguez's communications make clear that they intended for criminals to use Samourai to conceal their crime proceeds, were "disappointed" when criminals used competitor mixers (rather than Samourai) to conceal crime proceeds, and criticized competitor mixers for inadequately concealing crime proceeds, risking the users' arrests and incarceration. Rodriguez further actively encouraged and solicited sanctions evaders to use Samourai. And Hill not only repeatedly advertised Samourai on darknet markets, he operated his own directory of darknet markets which included links to a drug supplier and a weapons supplier.

The foregoing messages raise significant concerns about the defendants' respect for the law, and anti-money laundering and sanctions evasion laws, in particular. To take one more striking example: on September 20, 2023, Rodriguez expressed his knowledge of and lack of respect for federal criminal anti-money laundering laws. Specifically, in response to a third party's critique of a separate statute's $10,000 threshold reporting requirement for financial institutions, Rodriguez opined that members of Congress were "Sickos" for "invent[ing] a new crime called 'structuring' to go along with the newly invented crime of 'money laundering.'" By (a) characterizing Congress's long-standing criminal prohibition of money laundering as a "newly invented" crime, (b) attacking the legitimacy of the law and suggesting it is a made-up crime by placing "money laundering" in quotation marks, and (c) referring to the legislative drafters as "Sickos," Rodriguez confirmed his disdain for federal criminal money laundering laws.

[21] Hill's own expert confirms that the defendants pitched this presentation to Samourai investors in 2015. (Dkt. 155 at 83, 84 n.5, 87 (citing "USAO_WH_00000024" as a "2015 Samourai investor presentation")).

Likewise, in response to law enforcement highlighting Samourai as a "top threat" to its ability to trace the proceeds of criminal activity, Hill wrote, "Europol also highlighted Samourai Wallet as an emerging 'top threat' in same article. Do you see us shitting in our pants ?" (PSR ¶ 34). Rodriguez publicly commented that he would "rather sit in a jail cell than comply with" AML requirements. (PSR ¶ 42).

All these messages demonstrate that that Rodriguez and Hill were well aware of the potential consequences of operating Samourai's money laundering service but nonetheless chose to commit the crime anyway.

In light of the severity, duration, and breadth of their conduct, coupled with the lack of any need or justification for their crimes and apparent disrespect for the law, specific deterrence and the need to promote respect for the law also weigh in favor of the Stipulated Guidelines Sentence of 60 months.

4. The Substantial Need to Generally Deter Money Laundering Using Cryptocurrency, Fiat Currency, and Other Mechanisms Such as Trade-Based Money Laundering Calls for a Sentence of 60 Months of Imprisonment

The need for general deterrence is paramount in this case, given how lucrative the illegal transmission of crime proceeds—especially cryptocurrency proceeds—can be. It is further necessary because of how difficult and resource-intensive it is to detect and prosecute illegal money transmission of crime proceeds, particularly illegal transmission of cryptocurrency that is frequently held in anonymous wallets, and the underlying crimes that transmission promotes and conceals.

One of the critical factors that the Court must consider in imposing sentence under Section 3553(a) is the need for the sentence to "afford adequate deterrence to criminal conduct." 18 U.S.C.

§ 3553(a)(2)(B). Courts have generally recognized that "white collar crime . . . requires heavy sentences to deter because it is potentially very lucrative." *United States v. Hauptman*, 111 F.3d 48, 52 (7th Cir. 1997); *see also Harmelin v. Michigan*, 501 U.S. 957, 988 (1991) (noting that "since deterrent effect depends not only upon the amount of the penalty but upon its certainty, crimes that are less grave but significantly more difficult to detect may warrant substantially higher penalties"). "Because economic and fraud-based crimes are more rational, cool, and calculated than sudden crimes of passion or opportunity, these crimes are prime candidates for general deterrence." *United States v. Martin*, 455 F.3d 1227, 1240 (11th Cir. 2006) (internal quotation omitted). "Defendants in white collar crimes often calculate the financial gain and risk of loss, and white collar crime therefore can be affected and reduced with serious punishment." *Id.*; *see also United States v. Goffer*, 721 F.3d 113, 132 (2d Cir. 2013) (noting district court's comments during an insider trading sentencing that defendant made a "deliberate decision, weighing the risks, that insider trading 'was a game worth playing'" and characterizing "district court's assertion that insider trading requires high sentences to alter that calculus" as "a Congressionally-approved example of giving meaning to the 18 U.S.C. § 3553(a) factors"); *United States v. Heffernan*, 43 F.3d 1144, 1149 (7th Cir. 1994) ("Considerations of (general) deterrence argue for punishing more heavily those offenses that either are lucrative or are difficult to detect and punish, since both attributes go to increase the expected benefits of a crime and hence the punishment required to deter it.").

This is particularly so, as here, in the case of sophisticated, profitable illegal money transmitting businesses involving the transmission of funds that are known to the defendants to have been derived from a criminal offense or are intended to be used to promote or support

unlawful activity. These types of crimes are pernicious and lucrative: they are extremely enriching to their perpetrators and yet inherently difficult for law enforcement to detect and stop. The prevalence of darknet markets has fueled criminal activity on a large scale. And decentralized finance hacks caused an astonishing $53.5 billion in losses in 2022 and well over $1 billion in annual losses in every year since.[22] Law enforcement relies on its ability to track cryptocurrency transactions to investigate and prosecute crimes ranging from drug transactions to darknet CSAM offenses. As these numbers above reveal, it has, unfortunately, become far too easy for cyber-criminals to profit on darknet marketplaces and/or target and victimize lawful businesses and their end users from behind computer screens, and to further hide their criminal proceeds through a web of concealment-focused transactions and mixers, such as Samourai.

The sentences the Court imposes on Rodriguez and Hill should send a strong and clear message to others that agreeing to transmit, and in fact transmitting known crime proceeds—regardless of the technology used or whether the proceeds are in the form of fiat or cryptocurrency—will be met with serious consequences, particularly when it facilitates crimes as crushing to victims as those illegally transmitted by Samourai.

---

[22] *See, e.g.*, Jeff Owens, *DeFi Has a Risk Problem and It's Time to Solve It*, CoinDesk, Dec. 20, 2023 (updated Dec. 20, 2023), https://www.coindesk.com/opinion/2023/12/20/defi-has-a-risk-problem-and-its-time-to-solve-it; Mohammed Khalil, *Crypto Hacking Incidents Statistics 2025: Losses, Trends*, DeepStrike, Oct. 24, 2025, https://deepstrike.io/blog/crypto-hacking-incidents-statistics-2025-losses-trends; Bessie Liu, *The 5 biggest DeFi hacks of 2023*, Blockworks, Dec. 22, 2023, https://blockworks.co/news/biggest-defi-hacks-2023; *see also* Zeke Faux, *Number Go Up* 102 (2023) (estimating that in 2021 a total of $3.2 billion in cryptocurrency was stolen from exchanges and decentralized finance apps).

5. A Sentence of 60 Months' Imprisonment Does Not Create Unwarranted Sentencing Disparities

Additionally, the Stipulated Guidelines Sentence of 60 months is appropriate to avoid creating an unwarranted sentencing disparity. As the Second Circuit has explained, "we have repeatedly made clear that 'section 3553(a)(6) requires a district court to consider nationwide sentence disparities, but does not require a district court to consider disparities between co-defendants.'" *United States v. Ghailani*, 733 F.3d 29, 55 (2d Cir. 2013) (quoting *United States v. Frias*, 521 F.3d 229, 236 (2d Cir. 2008)). "The best way to curtail 'unwarranted' disparities is to follow the Guidelines, which are designed to treat similar offenses and offenders similarly." *United States v. Bartlett*, 567 F.3d 901, 908 (7th Cir. 2009).

Here, the Presentence Reports' summary of the U.S. Sentencing Commission's Judiciary Sentencing Information data, which analyzed the sentences imposed over the last five fiscal years (FY2020-2024) on the 64 defendants whose primary guideline was § 2S1.1, with the same final offense level, 35, and Criminal History Category, I, as Rodriguez and Hill, indicates that the average sentence imposed was 109 months and the median sentence imposed was 120 months. (PSR ¶ 34). Accordingly, to sentence Rodriguez and Hill below 60 months—itself already half of the median sentence imposed on similarly situated defendants—would risk creating an unwarranted sentencing disparity.

For his part, Hill primarily cites a number of inapt cryptocurrency cases that largely, unlike here, do not involve the transmission of *known* criminal proceeds and the U.S.S.G. § 2S1.1 guideline, but instead involve the irrelevant U.S.S.G. § 2S1.3 registration offenses of failing to get a money transmission license and violating the Bank Secrecy Act. As noted above, such failure-to-register offenses are not at issue here and have lower offense levels than those subject to the

U.S.S.G. § 2S1.1 guideline that the parties agree applies. *See* Hill Subm. 43-44 (citing the *Hayes* BitMEX and *Zhou* Binance cases). Notably uncited in Hill's submission was the 12.5 year sentence, following his trial conviction, of Roman Sterlingov, the operator of the Bitcoin Fog cryptocurrency mixer. *See United States v. Roman Sterlingov*, No. 21 Cr. 399 (RDM), (D.D.C. Nov. 8, 2024), Dkt. 340 (Judgment). Unlike Rodriguez and Hill, whose mixer transmitted over $2.3 billion in virtually untraceable transactions of which, conservatively, at least $237 million were criminal proceeds, Sterlingov's mixer transmitted a smaller but still quite large volume of transactions: over $400 million in virtually untraceable transactions of which, conservatively, at least $67 million were criminal proceeds. *Id.*, Dkt. 314 at 31-32 (Gov't Sent. Memo). That defendant nonetheless received a sentence much greater than that requested here.[23]

Likewise, in this Court's sentencing of Liberty Reserve founder Arthur Budovsky, significant portions of the offense conduct resemble Rodriguez and Hill's conduct here, and the Court ultimately imposed a sentence of 20 years' imprisonment. *See United States v. Arthur Budovsky*, No. 13 Cr. 368 (DLC), (S.D.N.Y. May 6, 2016), Dkt. 382 (Sentencing Tr.). As this Court observed at sentencing in that case, the illegal business there, like Samourai:

> was designed to be used by cyber criminals, and it was, to hide and move their ill-gotten gains. It was designed to appeal to them, and it did. It was successful in capturing a very significant share of this international business. There were over 78 million financial transactions processed by Liberty Reserve. The combined value was over $8 billion. This money laundering for criminal activity had a huge U.S. footprint. The parties have agreed that at least a quarter of a billion dollars in criminal proceeds from user accounts based in the United States went through the Liberty Reserve system.

[23] Unlike Rodriguez and Hill, Sterlingov went to trial and contested the majority of facts surrounding his offense conduct, including those underlying the Guidelines enhancements to which he agreed, resulting in protracted arguments at sentencing regarding the scope of the offense conduct.

. . .

> The challenges are enormous in this digital age of having effective law enforcement in this kind of e-currency market and money-laundering scheme. So there is an enormous importance to thinking about general deterrence here.

Id. at 46, 54. Also applicable to Rodriguez and Hill's sentencings, this Court explained at Budovsky's sentencing the damage third-party money laundering causes to victims of the underlying offenses, when it observed that Budovsky's money-laundering operation "facilitated, encouraged, [and] assisted in significant ways" the underlying frauds and "empowered, enabled, facilitated other fraudsters around the world." *Id.* at 47, 52; *see also id.* at 48 ("[L]ooking at this crime and these facts, and the defendant's role in it, looking at the extent of lives impacted, destroyed, changed forever, the lost savings, the lost retirement funds, the emotional distress, the loss of self-respect, the recriminations, the strain in family life, they're all appropriately captured, I think, through this guidelines application."); *id.* at 53 ("Mr. Budovsky has used his enormous talents here in a way that has led to widespread harm, countless victims of fraud around the world, many, many, many in the United States, ...").

While Sterlingov and Budovsky, a recidivist offender, may not be perfect comparators to the defendants, they show that defendants who engaged in long-running criminal schemes involving the knowing transmission of hundreds of millions in crime proceeds have repeatedly received sentences far steeper than the Stipulated Guidelines Sentence and statutory maximum sentence here of 60 months. The far below-Guidelines sentences requested by Hill and Rodriguez would result in gross and unwarranted sentencing disparities that Section 3553 specifically instructs to avoid.

6. The Court Should Impose a Fine

Finally, the Government agrees with the Probation Office that a fine is appropriate and that both defendants have the ability to remit a fine. (PSR-R ¶¶ 38, 40; PSR-H ¶¶ 36, 38). However, whereas the Probation Office recommends a fine of $20,000 for each defendant—half of the bottom of the Guidelines fine range of $40,000—the Government respectfully seeks a fine at or near the top of the Guidelines range of $250,000. Such a fine is appropriate given the defendants' harmful and lucrative offense conduct and their ability to pay, including their possession of over two BTC each, valued today at over $218,000 per defendant, and the fact that the approximately 246.3 BTC the defendants earned in fees from Samourai is valued today at over $26.9 million. (PSR-R ¶ 101; PSR-H ¶ 109).

IV. CONCLUSION

The Stipulated Guidelines Sentence of 60 months' imprisonment is an appropriate and just sentence for each respective defendant. Such a sentence would recognize the breadth and seriousness of the defendants' long-running offense. By contrast, a sentence involving less than 60 months would fail to adequately account for the scope of the harm caused by Rodriguez and Hill's largescale concealment of crime proceeds and promotion and support of serious, devastating crimes.[24]

Dated: New York, New York
October 31, 2025

Respectfully submitted,

NICOLAS ROOS
Acting Deputy United States Attorney
Attorney for the United States
Acting Under Authority Conferred by
28 U.S.C. § 515

By: /s/
Andrew K. Chan / David R. Felton
Cecilia E. Vogel
Assistant United States Attorneys
Tel: 212-637-1072 / 2299 / 1084

cc: Defense counsel (by ECF)

[24] The Government also respectfully requests that the Court orally impose forfeiture at sentencing, consistent with the consent forfeiture orders previously entered. (Dkt. 142, 143). Restitution is not applicable. As for supervised release, in light of recent Second Circuit decisions, the Government respectfully requests that, for each special condition of supervised release that the Court intends to impose, the Court briefly state its reasons for concluding that each such special condition is "reasonably related" to at least one of the factors set forth in U.S.S.G. § 5D1.3(b). *See, e.g.*, *United States v. Sims*, 92 F.4th 115 (2d Cir. 2024) (vacating special condition and remanding for district court to provide sufficient explanation for imposition of condition); *United States v. Oliveras*, 96 F.4th 298 (2d Cir. 2024) (same); *United States v. Jimenez*, No. 22-1022, 2024 WL 1152535 (2d Cir. Mar. 18, 2024) (summary order) (same).