

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

-----X
 :
 UNITED STATES OF AMERICA :
 :
 - v. - :
 :
 VIRGIL GRIFFITH, :
 :
 Defendant. :
 :
 -----X

20 Cr. 15 (PKC)

GOVERNMENT’S SENTENCING MEMORANDUM

DAMIAN WILLIAMS
United States Attorney
Southern District of New York

Kimberly J. Ravener
Kyle A. Wirshba
Assistant United States Attorneys
- Of counsel -

TABLE OF CONTENTS

TABLE OF CONTENTS..... i

TABLE OF AUTHORITIES i

PRELIMINARY STATEMENT 1

BACKGROUND 2

 A. The U.S. Sanctions Regime Relating to North Korea..... 2

 B. Griffith’s Participation in the Sanctions Evasion Conspiracy..... 5

 1. Griffith’s Initial Attempts to Develop Cryptocurrency Infrastructure Inside the DPRK 6

 2. Griffith Secures a Spot at the Conference 12

 3. Griffith’s Attendance and Presentations at the Conference 16

 4. Griffith’s Other Activity During the April 2019 Trip to the DPRK 27

 5. Griffith’s Statements to Law Enforcement after the Conference 32

 6. Griffith Continues to Pursue the Advancement of DPRK Cryptocurrency Services..... 34

 C. Griffith’s Guilty Plea..... 39

 D. The Presentence Report and Defense Submission 39

DISCUSSION..... 40

 I. Applicable Law 40

 II. A Guidelines Incarceratory Sentence and Fine Are Warranted 41

 A. The Seriousness of the Offense and Need to Promote Respect for the Law 42

 B. The Need for Deterrence 47

 C. The Court Should Impose a Substantial Guidelines Fine 50

 D. Griffith’s Sentencing Arguments Do Not Warrant a Reduced Sentence 52

 1. Griffith’s Contacts with Law Enforcement Do Not Mitigate His Conduct 52

 2. Griffith’s Commission of the Crime For Free Fails to Mitigate His Conduct..... 56

 3. Griffith’s Offense Exceeded “Providing Publicly Known Oral Information” 57

 4. Comparable Sentences 61

CONCLUSION..... 64

TABLE OF AUTHORITIES

Cases	Page(s)
<i>Gall v. United States</i> , 552 U.S. 38 (2007)	40
<i>Massie v. Gov’t of Democratic People’s Republic of Korea</i> , 592 F. Supp. 2d 57 (D.D.C. 2008)	4, 7, 11
<i>Sarvestani v. United States</i> , 2015 WL 7587359 (S.D.N.Y. Nov. 25, 2015)	61
<i>McMorris v. Carlos Lopez & Assocs., LLC</i> , 995 F.3d 295 (2d Cir. 2021)	15
<i>United States v. Amirnazmi</i> , 645 F.3d 564 (3d Cir. 2011)	62, 63
<i>United States v. Banki</i> , 685 F.3d 99 (2d Cir. 2012)	62
<i>United States v. Salameh</i> , 261 F.3d 271 (2d Cir. 2001)	50, 51
<i>United States v. Ulbricht</i> , 858 F.3d 71 (2d Cir. 2017)	11, 12
<i>Warmbier v. Democratic People’s Republic of Korea</i> , 356 F. Supp. 3d 30 (D.D.C. 2018)	4
 Statutes	
18 U.S.C. § 1544	13, 15
18 U.S.C. § 3553	<i>passim</i>
50 U.S.C. § 1701	2
50 U.S.C. §§ 1701	2
Section 5K1.1	61
Section 3553	40, 52
 Other	
22 C.F.R. § 51.62	13
31 C.F.R. Part 510	2

supra 8 56
U.S.S.G. § 5E1.2 50

PRELIMINARY STATEMENT

The Government respectfully submits this memorandum in connection with the sentencing of defendant Virgil Griffith (“Griffith” or the “defendant”), currently scheduled for April 12, 2022.

The U.S. Government relies on sanctions as a critical means of protecting our national security. Sanctions are a key tool for mitigating and deterring threats from our nation’s adversaries, without resorting to military force. Evading sanctions serves to undermine the U.S. Government’s ability to use diplomacy in the face of potential conflict, rogue actors, and in the case of North Korea, a nuclear threat. Teaching our adversaries how to subvert sanctions – which is precisely what the defendant did in this case with North Korea – is gravely serious conduct that jeopardizes the efficacy of the sanctions regime and endangers the public.

Griffith is an American citizen who chose to evade the sanctions of his own country to provide services to a hostile foreign power. He did so knowing that power – North Korea – was guilty of atrocities against its own people and has made threats against the United States citing its nuclear capabilities. He traveled to North Korea knowing not only that he was illicitly delivering a service in violation of sanctions, but also that his valuable cryptocurrency expertise would be itself used by North Korea for the purpose of sanctions evasion. And this trip was only part of a years-long endeavor by the defendant to do business with and assist North Korea. Despite Griffith’s self-serving rationalizations, these actions did not further world peace, they were not lacking in seriousness, and they cannot be excused or explained by the defendant’s claimed medical issues and impulsivity. The defendant persistently worked, over an extended period, to advance his cryptocurrency business by serving the interests of one of America’s most dangerous and volatile adversaries, and his conduct threatening U.S. national security requires serious consequences.

For these actions, a substantial sentence within the Guidelines range of 63 to 78 months' imprisonment is necessary to reflect the nature and seriousness of the offense, to promote respect for the law, and to deter others, especially those who would also seek to advance their own interests by serving hostile foreign powers at the expense of our collective national security. A fine towards the top of the Guidelines range – \$1,000,000 – is also warranted to deter the defendant and others from similar conduct in the future.

BACKGROUND

A. The U.S. Sanctions Regime Relating to North Korea

The International Emergency Economic Powers Act (“IEEPA”), 50 U.S.C. §§ 1701 *et seq.*, authorizes the President “to deal with unusual and extraordinary threat[s] . . . to the national security, foreign policy, or economy of the United States” by declaring a national emergency with respect to such threats, and to take steps to address such threats. 50 U.S.C. § 1701(a). Beginning in 2008, with the issuance of Executive Order 13466, the President declared a national emergency with respect to the threats posed by North Korea to the United States’ national security and foreign policy, and directed certain measures to respond to that emergency.

Pursuant to these declarations and directives, the U.S. Department of Treasury’s Office of Foreign Assets Control (“OFAC”) promulgated the North Korea Sanctions Regulations (“NKSR”) to implement sanctions on the Democratic People’s Republic of Korea (“North Korea” or “DPRK”). *See* 31 C.F.R. Part 510. At all times relevant to this case, the NKSR prohibited, among other things, the “exportation or reexportation, directly or indirectly, from the United States, or by a U.S. person, wherever located, of any goods, services, or technology to North Korea” and “[a]ny conspiracy formed to violate the prohibitions set forth in this part.” 31 C.F.R. §§ 510.206(a), 510.212(a)-(b).

Between 2008 and 2017, the President identified the DPRK's repeated tests of nuclear weapons and intercontinental ballistic missile launches, its "unprovoked attack that resulted in the sinking of the Republic of Korea Navy ship Cheonan and the deaths of 46 sailors in March 2010," "its illicit and deceptive activities in international markets through which it obtains financial and other support, including money laundering, the counterfeiting of goods and currency, bulk cash smuggling, and narcotics trafficking," and its "destructive, coercive cyber-related actions," among other DPRK policies and actions, as extraordinary threats to the United States.¹ As a result of this national emergency, which has been continuously in effect at all times relevant to this case and remains today, the President established a comprehensive embargo on the DPRK. A core purpose of the sanctions has been to compel the DPRK's regime to change its behavior in the international community. Griffith's conduct served to undermine that national security objective.

At all times relevant to the defendant's conduct, North Korea was also designated by the U.S. State Department as a state sponsor of terrorism² and repeatedly cited for its human rights atrocities against its own citizens and others. As the District Court for the District of Columbia has observed, based on expert testimony regarding the DPRK regime:

North Korea is the "most advanced, most perfected totalitarian state in world history," and has "perfected its means of terrorizing" both its own people and others. The dictator who leads North Korea, and his cronies, "show[] no regard for human life," creating, for example, a "manmade . . . famine" in the late 1990s that killed "upwards of 2 million people," and maintaining "political prisoner concentration camps," such that "North Korean escapees" tell "a consistent story" of "a life of extreme deprivation and repression." Moreover, North Korea is "unprecedented" in its state

¹ See Notice on the Continuation of the National Emergency with Respect to North Korea, *available at* <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/06/21/notice-on-the-continuation-of-the-national-emergency-with-respect-to-north-korea/> (last visited []).

² See U.S. Department of State, State Sponsors of Terrorism, *available at* <https://www.state.gov/state-sponsors-of-terrorism/> (last visited Nov. 3, 2021) (citing North Korea's designation as of Nov. 20, 2017).

sponsorship of “[il]licit activities, like proliferation of weapons of mass destruction, counterfeiting U.S. dollars, [and] the production and sale of drugs like opium, heroin, and meth[amphetamines].”

Warmbier v. Democratic People’s Republic of Korea, 356 F. Supp. 3d 30, 36 (D.D.C. 2018) (internal citations omitted). U.S. federal courts have held North Korea liable “for the torture, hostage taking, and extrajudicial killing of Otto Warmbier,” an American college student, *id.* at 60, and the torture and hostage taking of U.S. Navy personnel, *Massie v. Gov’t of Democratic People’s Republic of Korea*, 592 F. Supp. 2d 57, 66 (D.D.C. 2008).

Since at least 2017, the North Korean government has publicly represented that it possesses the capability to target the continental United States with a nuclear warhead.³ The potential nuclear threat posed by North Korea persisted throughout the pendency of this case. Based on public reporting, North Korea tested a nuclear weapon in September 2017, prompting the U.S. to warn of a “a massive military response,”⁴ was caught clandestinely advancing its nuclear program in November 2018,⁵ and conducted three missile tests, including a new hypersonic missile, a new cruise missile, and a train-launched ballistic missile system, as part of a five-year military development plan pursued in defiance of the United Nations in September 2021.⁶ U.S. and U.N.

³ See “North Korea Tests First Submarine-Launched Missile in Two Years,” *The New York Times* (Oct. 18, 2021), available at <https://www.nytimes.com/2021/10/18/world/asia/north-korea-ballistic-missile-test-washington.html> (last visited Mar. 18, 2022).

⁴ “North Korean Nuclear Test Draws U.S. Warning of ‘Massive Military Response,’” *New York Times* (Sept. 3, 2017), available at <https://www.nytimes.com/2017/09/03/world/asia/north-korea-tremor-possible-6th-nuclear-test.html> (last visited Mar. 18, 2022).

⁵ See “In North Korea, Missile Bases Suggest a Great Deception.” *New York Times* (Nov. 12, 2018), available at <https://www.nytimes.com/2018/11/12/us/politics/north-korea-missile-bases.html> (last visited Mar. 18, 2022).

⁶ See “North Korea says it fired new ‘hypersonic missile,’” *BBC News* (Sept. 29, 2021), available at <https://www.bbc.com/news/world-asia-58729701> (last visited Mar. 18, 2022).

sanctions play an important role in attempting to curb the North Korean regime's malicious behaviors, and especially its nuclear program. Over time, U.S. and international economic sanctions have focused on attempting to isolate North Korea and the North Korean economy from the international financial sector and international economy, to push the regime to stop threatening a nuclear war and otherwise committing atrocities against its citizens and others, while offering the opportunity for diplomacy.

B. Griffith's Participation in the Sanctions Evasion Conspiracy

Beginning as early as February 2018, the defendant plotted with others to illegally provide services to the DPRK and DPRK persons, without a license and in contravention of the North Korean sanctions, by (1) developing cryptocurrency infrastructure and equipment inside North Korea, including to mine cryptocurrency; (2) traveling to the DPRK, in coordination with the DPRK government, to present at the April 2019 Pyongyang Blockchain and Cryptocurrency Conference (the "Conference"); (3) assisting individuals inside the DPRK seeking to evade and avoid U.S. sanctions through, among other things, particular cryptocurrency transactions; (4) developing plans to create specialized "smart contracts" to serve the DPRK's unique interests; (5) attempting to aid the DPRK to engage in cryptocurrency transactions; and (6) attempting to broker introductions for the DPRK to other cryptocurrency service providers. During the Conference in particular, Griffith and his co-conspirators provided services to approximately 100 North Korean attendees by advising on how they could use cryptocurrency technology to evade sanctions, pitching financial services involving blockchain technology to the DPRK attendees, and consulting with DPRK citizens on ways to transfer cryptocurrency assets, among other things. Upon his return from the Conference, Griffith continued his efforts to provide these services to the DPRK, and attempted to recruit others with cryptocurrency expertise to do the same.

The evidence collected in the case included Griffith's emails and other messages found on his digital devices and electronic accounts, statements of the defendant to law enforcement, social media posts and messages, photographs, audio recordings, video of the Conference from inside the DPRK, and law enforcement and civilian witness testimony, as reflected in the facts set forth below.

1. Griffith's Initial Attempts to Develop Cryptocurrency Infrastructure Inside the DPRK

The defendant, a cryptocurrency expert, began formulating plans as early as February 2018 to aid individuals in the DPRK in developing cryptocurrency infrastructure there. PSR ¶ 16.⁷ At the time, Griffith, an American citizen, was living in Singapore and employed as the "Head of Special Projects" and a "Senior Researcher" at the Ethereum Foundation, an international cryptocurrency organization and creator of a cryptocurrency bearing the same name (ether). PSR ¶ 14. Griffith was one of the few individuals who held a title within the Ethereum Foundation, where he worked at closely with Ethereum's founder and a small group of others at the top level of the organization. (*See* 3521-01.) Griffith's responsibilities at Ethereum included business development. As early as February 17, 2018, Griffith proposed a plan to provide cryptocurrency services in the DPRK to a Singaporean contact ("CC-3")⁸ who was scheduled to travel to the DPRK for a marathon. Griffith wrote, in an electronic message, "[i]f you find someone [in North Korea], we'd love to make an Ethereum trip to DPRK and setup an Ethereum node."⁹ PSR ¶ 18.

⁷ In this memorandum, "Probation" refers to the United States Probation Office; "PSR" refers to Probation's presentence investigation report; "GX__" refers to the Government's exhibits marked for trial; and "Def. Mem." refers to Griffith's sentencing memorandum dated March 4, 2022.

⁸ For ease of reference, the Government has used the same anonymized identifiers in this brief, including with respect to Griffith's co-conspirators, as used in prior filings in this case.

⁹ A "node" is a computer that connects to a cryptocurrency network that is responsible for validating and relaying cryptocurrency transactions. Depending on the cryptocurrency and type of

When CC-3 questioned whether the plan made “economic sense,” Griffith responded, “It does actually[.] It’ll help them circumvent the current sanctions on them.”¹⁰ *Id.* CC-3 agreed to assist. *Id.*

In April 2018, Griffith’s emails reflect that CC-3 connected Griffith by email to a British citizen working for a tour group (“CC-4”) who traveled frequently to North Korea. CC-3 described that “Virgil is the Ethereum guy who would like to get the node . . . started.” On April 6, 2018, Griffith responded to CC-4 that he was “willing to spend up to 8k USD on this project,” presuming that “most of that will go into paying for internet/bribes,” and that he would “Buy the mining rig Ship it to them [and] Pay someone or some entity to continue maintaining it” PSR ¶ 19. Griffith wrote that, while he asked Ethereum management “if we’d directly do this,” he was told that, because of sanctions, only “doing so through an intermediary is possible.” PSR ¶ 20. Until they figured out the intermediary, however, Griffith wrote that the project “will be supported by myself, an individual.” PSR ¶ 20. Anticipating a potential issue due to the sanctions, Griffith acknowledged that he was “a US citizen, but I’ll be funnelin[g] things through Singapore/China to avoid any problems from that.” PSR ¶ 20. Griffith ended the email by noting, “if this works out I know a few other decentralized networks that would love to have a node in DPRK. This could turn into a mildly lucrative little business for whoever does this.” PSR ¶ 20.

CC-4 responded that day with some skepticism, noting that setting up a node in the DPRK would be “incredibly difficult.” PSR ¶ 21. CC-4 advised Griffith via email that such

node, a computer acting as a node is often rewarded for the validation it undertakes with additional cryptocurrency, in a process called “mining.” An individual running a node, therefore, might also receive cryptocurrency as part of the process.

¹⁰ Communications quoted herein appear as in the original unless otherwise indicated. Quotations from audio and video recordings are based on draft transcriptions.

a project would require in-person meetings in the DPRK, which Griffith could not undertake, and that CC-4 would need to get permission from the British Embassy given the likely sanctions implications. PSR ¶ 21.

Griffith was undeterred. PSR ¶ 21. The next day, on April 7, 2018, Griffith wrote CC-4 to further market the plan: “Another benefit of an Ethereum node in dprk . . . It’ll make it possible for them to avoid sanctions on money transfer. This seems like something that would interest them.” PSR ¶ 22. Griffith followed up days later, on April 9, 2018, writing that he would “update my maximum spend on this to \$10,000 USD. I really hope we can make this work!” PSR ¶ 22. On April 14, 2018, Griffith offered added incentives: “Also, If you’re able to make this happen, I’d be delighted to pay you a generous consulting fee.” PSR ¶ 22.

On a parallel track, on June 30, 2018, Griffith emailed a South Korean business contact (“CC-5”) to seek her assistance in pursuing a cryptocurrency node in the DPRK as well. PSR ¶ 23. Around this time, Griffith was working to negotiate a contract to hire CC-5 and CC-5’s company to perform services for Ethereum, including, as Griffith wrote, “[s]eeking for and introducing potential business partners or personnel to the Company.” PSR ¶ 23. In an email to Griffith, CC-5 asserted that the South Korean government was “open to providing support to the Ethereum Foundation,” and that “supporting an Ethereum research center and setting up an institution at DPRK came up.” PSR ¶ 23. Griffith responded, “To be clear an ‘institution’ in DPRK isn’t needed---just an Ethereum node from a registered dprk ip block. If DPRK wants to do more beyond that, that’s great too.” PSR ¶ 23. On July 4, 2018, CC-5 followed up with Griffith and his colleagues, stating that “the NK [North Korea] node idea was considered, but Gaeseong Industrial Complex in NK wishes to focus on producing material goods for now. So the idea needs to be held off for a

bit, but I think it may be feasible in the longer term.” PSR ¶ 23.

Approximately one month later, on August 7, 2018, CC-4 updated Griffith by email, stating in an email to Griffith that “It’s been many months, and many meetings, but we finally have news of progress for you . . . we are in talks with [North] Koreans at the Internet company in Pyongyang who will be able to get this node online for you.” PSR ¶ 24. As described by CC-4, Griffith would need to “register as a Joint Venture” and “pay for three technical staff (3 x 8 hour shifts) to monitor the computer.” PSR ¶ 24. Griffith responded, “Is there a minimum of hiring 3 people? If so, we’ll try to find additional things [for] them to do. Maybe running a Korean language wiki. Or maybe have them work at setting up a crypto exchange in DPRK-that might be too adventurous.” When CC-4 responded that the three employees were mandatory, Griffith wrote, “Any suggestions on how to deal with sanctions related issues?” PSR ¶ 24. It appears that CC-4 did not respond in writing. PSR ¶ 24. The same day, Griffith messaged CC-3, “Do you got a lawyer who is familiar with sanctions laws on DPRK? [CC-4] got back to me[.] Will try and setup a dprk shell company.” PSR ¶ 24. In response, CC-3 wrote, “One step closer.” PSR ¶ 24.

The same day he received the above-described August 7, 2018 email from CC-4, Griffith bragged about his progress to CC-5 via WhatsApp, writing, “I’ve gotten news from dprk[.] They are open to an Ethereum node . . . If we do the dprk thing, can you help with the shell company to do it?” PSR ¶ 25. That same day, Griffith also forwarded CC-4’s email to the co-founder of the Ethereum Foundation and Griffith’s ultimate boss (“Individual-1”), and another Ethereum Foundation leader (“Individual-2”). PSR ¶ 25. Individual-1 and Individual-2 appear to have discouraged Griffith from proceeding with the node. PSR ¶ 25. On August 17, 2018, Griffith wrote to Individual-1, “I’ve decided to not actively pursue the dprk node. I decided you two [Individual-1 and Individual-2] were right that this was too risky.” PSR ¶ 26. But in fact, Griffith did no such

thing, and continued pursuing the scheme. PSR ¶ 26.

On August 24, 2018, Griffith continued to advance the project while simultaneously paying lip service to the sentiment apparently expressed by his company's leadership that he should not pursue it. PSR ¶ 26. He wrote CC-5,

I also wanted to ask about the DPRK node. [Ethereum Foundation] has to back away from it, but if South Korea wants to curry our favor, getting a way to send funding for such a thing to dprk would be immensely appreciated. We would do it myself/ourselves but we are scared of the sanctions. It seems to me that South Korea is allowed to violate those sanctions. The person who got the okay from the dprk ISP is [CC-3's email address]. I've been asked to step away from this project. So alas I must do that[.] But if you ever see a lead to do this, we'd love you for it.

When CC-5 replied, “[F]or the DPRK issue, it is quite sensitive so I have to be careful too[.]”

Griffith responded, “Awesome[.] I'm glad you're treating it as sensitive[.] That's exactly what I want[.]” PSR ¶ 27.

Griffith also began researching travel to the DPRK. PSR ¶ 28. On August 26, 2018, Griffith wrote an email to korea@korea-dpr.info (the “DPRK Email Account”) from his Ethereum email account, asking, “Can American citizens attend the blockchain conference?” PSR ¶ 28. An email address with the username “Special Delegation-DPR of Korea” sent a response stating, “Yes, no problem.” PSR ¶ 28. Griffith responded: “Wait really? I presumed that was impossible. Have American citizens previously visited under similar programs?” PSR ¶ 28. The sender answered, “No. It is the first time.” PSR ¶ 28. The next day, Griffith contacted by email CC-2, a cryptocurrency professional and, as described further below, one of the organizers of the Conference, who advised Griffith that “the dprk will not stamp your passport” if Griffith elected to travel to the Conference. PSR ¶ 28.

Griffith next made plans to travel to North Korea, and discussed his plans to participate in

the Conference. PSR ¶ 29. On August 31, 2018, one of Griffith's friends ("Individual-3") asked in an email exchange why Griffith was willing to risk his safety to go to a conference in the DPRK. PSR ¶ 28. Griffith expressed that he was unafraid of the DPRK authorities, because "DPRK wouldn't want to scare away Blockchain talent that'll let them get around sanctions." PSR ¶ 29. In response, Individual-3 asked, "What if they're funding their drug trade and nuclear program with crypto?" PSR ¶ 29. Griffith replied, "Unlikely. But they'd probably like to start doing such." PSR ¶ 29. In another messaging exchange with his parents and sister discussing the Conference, on November 26, 2018, Griffith acknowledged that the DPRK's interest in cryptocurrency was "probably avoiding sanctions . . . who knows." PSR ¶ 31. On September 12, 2018, Griffith corresponded with an individual about the Conference, who told Griffith they were "surprised that DPRK even has conferences." GX 2408. Griffith responded: "I presume they want to find ways to avoid sanctions." *Id.*

Nor did Griffith abandon his plans to establish a cryptocurrency mining node in the DPRK. Griffith instead redirected his efforts to find and enlist others willing to carry out the plans for him. On September 23, 2018, Griffith wrote to another individual affiliated with the Tor Project,¹¹ forwarding a message from CC-4 and stating:

I once mentioned to you the idea of doing a node in DPRK. I was going to put an Ethereum node there, but I eventually decided it was too edgy and decided against it. However, Tor doesn't mind being edgy in these ways. If Tor or others would like to crowdfund putting a Tor node in DPRK, I bet they'd do it under the same conditions described below.

¹¹ The Tor Project is a nonprofit organization with that maintains software for the Tor anonymity network. Tor is an acronym for "The Onion Router," "a special network on the Internet designed to make it practically impossible to physically locate the computers hosting or accessing websites on the network." *United States v. Ulbricht*, 858 F.3d 71, 83 (2d Cir. 2017).

If you got enough interest and willpower on your side (will require setting up a nonprofit in North Korea), I'm willing to make the introductions.

GX 3024. The forwarded message contained a list of the DPRK's requirements, including to "register as a Joint Venture," "paying rent," "pay[ing] for three technical staff," and a written proposal. Griffith redacted out CC-4's name and email address to hide CC-4's true identity. *Id.*

2. Griffith Secures a Spot at the Conference

On November 22, 2018, the DPRK Email Account extended a formal invitation for Griffith to "attend the Blockchain Conference in Pyongyang, DPR Korea, from Apr. 18th to Apr. 25th." PSR ¶ 30. The email included information about the Conference, a bank account to which the 800 Euro "booking fee" could be remitted, and a link to a website. PSR ¶ 30.

The linked website consisted of an advertisement for the "Pyongyang Blockchain and Cryptocurrency Conference" to be held on April 18 to 25, 2019. This advertisement contained a frequently asked questions ("FAQ") section and explained how to apply for the Conference by emailing a scan of a passport, name, address, telephone number, and short resume to DPRK Email Account. The FAQs noted, "The organizers of the conference are, in the DPRK side, [CC-1], Special Delegate for the Committee for Cultural Relations and president of the Korean Friendship Association (KFA), and in the technical side [CC-2]."

CC-1 is a Spanish national who holds a role linked to the DPRK government of Special Delegate for North Korea's Committee for Cultural Relations with Foreign Countries. PSR ¶ 32. CC-2 is a British citizen who worked for cryptocurrency and blockchain technology companies. PSR ¶ 32. According to the online Conference advertisement, CC-2 was a "Blockchain and Crypto expert." PSR ¶ 32. On November 23, 2018, CC-2 created a group chat to promote the Conference on an encrypted application, Telegram, and provided a website link to permit others to confirm their attendance (the "Encrypted Group Chat"). PSR ¶ 32.

On December 19, 2018, Griffith submitted his initial payment for the Conference and forwarded proof of the same to the DPRK Email Account. PSR ¶ 33. At all times relevant to the charged conduct, and as Griffith was aware as described below, U.S. law prohibited U.S. citizens from using a U.S. passport to travel to, in, or through North Korea without a special validation from the Department of State.¹² PSR ¶ 33. In preparation for his trip, on January 24, 2019, Griffith's WhatsApp communications reflect that he consulted with an individual who "has knowledge and experience in North Korea" ("Individual-4"). According to Griffith's WhatsApp messages with Individual-4, Individual-4 believed "there are good legitimate uses of blockchain in NK[.] But from the US perspective now at a time when sanctions are the forefront . . . [a]nything blockchain and NK will be seen as money laundering/ teaching sanctions circumvention [s]o it could get you tagged by USG in a not too favorable light. . . . Talk about entrepreneurship and business [b]ut not anything that helps circumvent sanctions." Despite this warning, Griffith continued to advance his plans to travel to North Korea and attend and present at the Conference, undeterred by the prospect of assisting North Korea to evade sanctions. In response to Individual-4, Griffith sent a thumbs up emoji and wrote, "sentence from my letter [to the State Department], 'I am aware of the sanctions on scientific exchange with the DPRK, and my talk will be solely on applications of blockchain technology for business and anti-corruption.'"

Griffith was referring to a letter he wrote to the State Department's Special Validations office on January 25, 2019, on the letterhead of a Singapore-based company (which was not his true employer), seeking permission to travel to the DPRK. PSR ¶ 15. In the letter, he stated, "I

¹² See, e.g., <https://travel.state.gov/content/travel/en/passports/how-apply/passport-for-travel-to-north-korea.html> (reflecting that travel to North Korea without a special validation "may justify revocation of your passport for misuse under 22 C.F.R. § 51.62(a)(2) and may subject you to felony prosecution under 18 U.S.C. § 1544 or other applicable laws").

have been accepted to speak at the Pyongyang Blockchain and Cryptocurrency Conference, and I wish to do so.” PSR ¶ 15. Griffith claimed that “[g]iven the sanctions on scientific exchange with the DPRK, my talk will be solely on the applications of blockchain technology to business and anti-corruption.” PSR ¶ 15. Griffith asserted that his trip would be “in the United States’ national interest,” because blockchain technology would enable “less corrupt services” in the DPRK, serve as a “neutral ground” for cooperation, provide “interactions between the DPRK and the rest of the world” that would be a “chink in the armor of the Kim regime,” and offered to “report back” if “DPRK representatives express interest in using blockchain technology to circumvent international sanctions.” The State Department denied Griffith’s application. PSR ¶ 15.

On January 27, 2019, Griffith wrote to CC-3 that he was going “[t]o meet with SGians [Singaporeans] who have business in dprk.” On February 14, 2019, Griffith received an email signed by CC-1 from the DPRK Email Account, bearing the subject, “Applying for blockchain conference,” and stating:

Because you have US passport, I already sent your data to my department in Pyongyang, the Committee for Cultural Relations with Foreign Countries. But they only can give the clearance after the first approval of our DPRK mission in NY. So, please communicate ASAP with: DPRK Mission to the U.N. E-mail: dpr.korea@verizon.net . . . Address: 820 Second Avenue, 13th Floor New York, NY 10017 USA[.] You have have to express your wish to participate in the blockchain conference from 18 to 25 April 2019, invited by the Committee for Cultural Relations with Foreign Countries. You can give the Reference/Contact person in Pyongyang: [Named DPRK official], Committee for Cultural Relations with Foreign Countries. You also have to send them your passport, personal details and CV (Resume).

GX 3036.

In response to the email from CC-1 and consistent with CC-1’s instructions, Griffith sent an email to “dpr.korea@verizon.net” on February 18, 2019, which included the following:

Hello to UN's DPRK Mission. I'm writing to you to request your permission to attend and speak at the blockchain conference from 18 to 25 April 2019. I have been invited by the Committee for Cultural Relations with Foreign Countries. My contact person in Pyongyang is: [Named DPRK official], Committee for Cultural Relations with Foreign Countries. I attach my passport, and CV.

GX 3037. The email address provided by CC-1, however, was incorrect. On February 28, 2019, Griffith received another email alerting him that "our NY mission was changed. Please send personal data, passport picture and request to visit in the following address: "DPRK.UN@VERIZON.NET." GX 3042. On March 7, 2019, Griffith forwarded his prior email to the correct email address, writing: "This is my request to visit the DPRK blockchain conference. See forwarded email below." GX 3044. Griffith also attached a picture of his passport and a digital link to his curriculum vitae, as CC-1 had directed would be necessary to procure "the first approval of our DPRK mission in NY." *Id.*

Griffith's curriculum vitae stated that "I mix novel technology and social insight to solve hard problems in legal tech, blockchains, and smart-contracts." The defendant identified approximately 10 computer programming languages, as well as "Tor" and "dark web,"¹³ among his proficiencies, described his work at Ethereum as including "developing decentralized VPN [virtual private network] system to replace Tor," and listed a host of his prior experiences in the

¹³ "The Dark Web is a general term that describes hidden Internet sites that users cannot access without using special software," namely, Tor. *McMorris v. Carlos Lopez & Assocs., LLC*, 995 F.3d 295, 302 n.4 (2d Cir. 2021) (quoting Kristin Finklea, Cong. Rsch. Serv., 7-5700, Dark Web 2 (2017) and further citing that "[n]ot surprisingly, criminals and other malicious actors . . . use the [D]ark [W]eb to carry out technology-driven crimes, such as computer hacking, identity theft, credit card fraud, and intellectual property theft." (Ahmed Ghappour, Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web, 69 Stan. L. Rev. 1075, 1090 (2017))).

self-described “Darkweb.” GX 610.

Around this same time, in March 2019, CC-1 posted to the Encrypted Group Chat, describing himself as the “[f]irst and only foreigner that works for the government of the DPRK.” CC-1 specifically indicated that he worked for the “Committee for Cultural Relations,” *i.e.*, the same DPRK government entity cited by Griffith in his email to the DPRK Mission in Manhattan. GX 201.

On April 17, 2019, approximately one month after contacting the DPRK Mission in Manhattan, Griffith received a visa to visit the DPRK, a copy of which he later posted to his Twitter account. PSR ¶ 34. Griffith subsequently admitted to law enforcement that he kept his visa separate from his passport in order to hide his travel to the DPRK from U.S. authorities. PSR ¶ 34.

3. Griffith’s Attendance and Presentations at the Conference

Griffith flew to the DPRK on April 18, 2019. PSR ¶ 35. The Conference occurred on April 23 and 24. PSR ¶ 35. Griffith departed the DPRK on April 25. PSR ¶ 35.

At the Conference, Griffith and his co-conspirators provided services to the DPRK attendees to facilitate sanctions evasion by: giving presentations on topics that had been pre-approved by DPRK officials, including cryptocurrency and blockchain technologies; teaching lessons to the Conference attendees and participants on blockchain and cryptocurrency technologies and their applications; answering questions about these technologies from Conference attendees and participants; providing advice in discussions regarding the potential uses for blockchain and cryptocurrency technologies to evade sanctions and launder money; pitching future cryptocurrency and blockchain services to the Conference attendees and participants,

including the creation of specialized smart contracts¹⁴ and the DPRK's own cryptocurrency coin; and acting as brokers to connect Conference attendees and participants with cryptocurrency equipment, service providers, and experts. PSR ¶ 36. Griffith was assigned a DPRK-government employee or handler responsible for the group's travel in the DPRK, as well as to control to whom they could speak, censor the photographs they took, and otherwise ensure compliance with the laws and policies of the DPRK ("CC-6"). PSR ¶ 37. Griffith later referred to CC-6 as a "minder" in his FBI interviews.

The events of the Conference were captured in part by audio recordings made by a witness on the first day of the Conference, video clips of the Conference and the defendant's remarks, notes written by Griffith for his presentation, images of Griffith giving presentations and writing on a whiteboard for the participants, including the below, and communications sent by Griffith to others during his time in the DPRK.

On the first day of the Conference, Griffith made the following statements, captured in an audio recording:

Hi everyone. My name is Virgil. I work for a group called the Ethereum Foundation. We do a sort of, next generation blockchain. I think the most valuable things we have to offer the DPRK are number one—we can give you, so blockchain gives you payments that the USA can't stop. And number two—we can give you contracts that don't go through the UN. So, if you make a contract with someone and the U.S. decides "oh, we don't want to do that anymore," you can still hold them to it. And that's kind of the two new things. Like before, if you send payments, you had to I guess, go through the U.S., and for international agreements, you had to go through the UN. With this new technology, you don't have to do that anymore and it's like, you know, great.

¹⁴ Smart contracts are computer programs built on a blockchain that allow for terms of an agreement to be enforced through, among other things, assets secured on a blockchain. *See* <https://www.coinbase.com/learn/crypto-basics/what-is-a-smart-contract>.

I suppose like one, not so good thing about this, is that the technology is still fairly new—maybe ten years told. So we haven't really, we don't really, like no one knows how to do all this right yet, but we definitely think this will be really useful for the DPRK, and that's why we're here. And if the DPRK adopts this, they will be on the very leading edge of technology.

During the same part of the Conference, CC-2 made the following statements, in the defendant's presence, to the Conference audience, which were also audio recorded:

So I'm going to outline now a way in which countries like Iran are now using blockchain in order to get around these sanctions that were placed on their banks.

So in summary, the blockchain for moving money around the world is not only very, very easy, especially for a count[r]y like the DPRK which has been imposed with the most horrific sanctions by the US government, but also it's quicker, faster, more safe, and easier.

CC-2 also described how the DPRK could potentially create its own cryptocurrency, and the potential advantages of doing so, stating:

So I'll give you an example. DPRK, I think would be the perfect example for creating its own stable coin. Why? It's because all of Korean won and all funds are held by one central bank under the economic system implemented in the DPRK. . . . So this would be exactly the same as buying and selling FX [foreign exchange] that you do right now—but without sanctions. So the exact same process but there would be no sanctions, or no reason to try and get around the sanctions. . . . And this would be a very easy process and something that could be built in a matter of weeks. It wouldn't be difficult and we're confident that with the number of experts in this room here with us today would be able to assist the central bank in implementing this.

Griffith was among the “experts in this room,” described by CC-2 as “able to assist.”

Another audio recording captured an additional portion of Griffith's presentation at the Conference, during which he made the following statements:

Hello everyone, I know it's late in the day so I'll try to make this fun. So the most important feature of blockchains is that they are

open. And the DPRK can't be kept out no matter what the USA or the UN says.

One of the more interesting things is that blockchains allow greater self-reliance in both banking and contracts. So you can have contracts without an authority. This is similar to a *juche*¹⁵ idea. . . .

So you've heard about with blockchain the USA can't stop your payments. So that's like step 1; step 2 is that the UN can't stop agreements. So if DPRK makes agreements with someone, or if an individual does, it's, you can, you don't have to go to a court.

[T]hat would suggest that if the DPRK wanted to explore this, would be to set up a small research group to study what kinds of contracts they would like to have all over the world that could be enforced on blockchain, not all of them can. But this is an active research area in science, actually no one really knows how to do this well yet, but y'all could be the first.

These remarks were consistent with Griffith's notes, recovered from a laptop that Griffith took with him to the DPRK. Those notes stated, "Blockchains are open-.DPRK can't be kept out," "[t]he USA won't be able to stop payments," and "[t]he UN won't be able to stop or cancel agreements." GX 808. Video footage from the Conference shows Griffith's DPRK handler, CC-6, giving him an approving "thumbs up" during this speech about the DPRK leveraging blockchain to evade sanctions "no matter what the USA or the UN says." GX 150.

Griffith spoke about the DPRK's use of nuclear weapons, including missiles in particular, at the Conference as part of the tailored services he provided and pitched to the DPRK audience. PSR ¶ 38. Griffith's notes for his "Blockchain and Peace" presentation describe "generic uses for

¹⁵ *Juche* is a Korean word that is roughly translated as "self-reliance" and is the "unique official philosophy" espoused by the North Korean regime with the "core idea that North Korea is a country that must remain separate and distinct from the world, dependent solely on its strength and the guidance of a near-godlike leader." *See* <https://www.vox.com/world/2018/6/18/17441296/north-korea-propoganda-ideology-juche>. Griffith returned from North Korea with an English language book "On the Juche Idea" by Kim Jong Il, the second "Supreme Leader" of the DPRK and the father of the current ruler.

DPRK” of blockchain technology, including “using smart-property to disable nukes based on upon fu[l]filled conditions.” PSR ¶ 38. This statement in Griffith’s notes refers to Griffith’s proposal, made at the Conference, that the DPRK could link the threat of a nuclear weapon, or choose to disable it (“disable nukes”), through smart contracts built upon blockchain technology. PSR ¶ 38. Recordings from the Conference reflect that Griffith in fact instructed the DPRK audience about the potential use of smart contracts in direct relationship to the DPRK’s nuclear missile program as follows:

Before you couldn’t hold a country accountable Like if it’s a big country. Like there’s nothing you could do. Now there is. So just an idea, so hypothetically you could have something where you could have a module on a missile, and the module could say something like you know if all the news reports say that sanctions on North Korea have been lifted, the missile will deactivate. But only then. And so this will give the U.S., I guess, confidence that Korea really will follow through to say that no no if you get rid of the sanction, the missile really are gone, like really. And so this is fundamentally a new way where they are automatic agreements you can’t take back.

. . . .

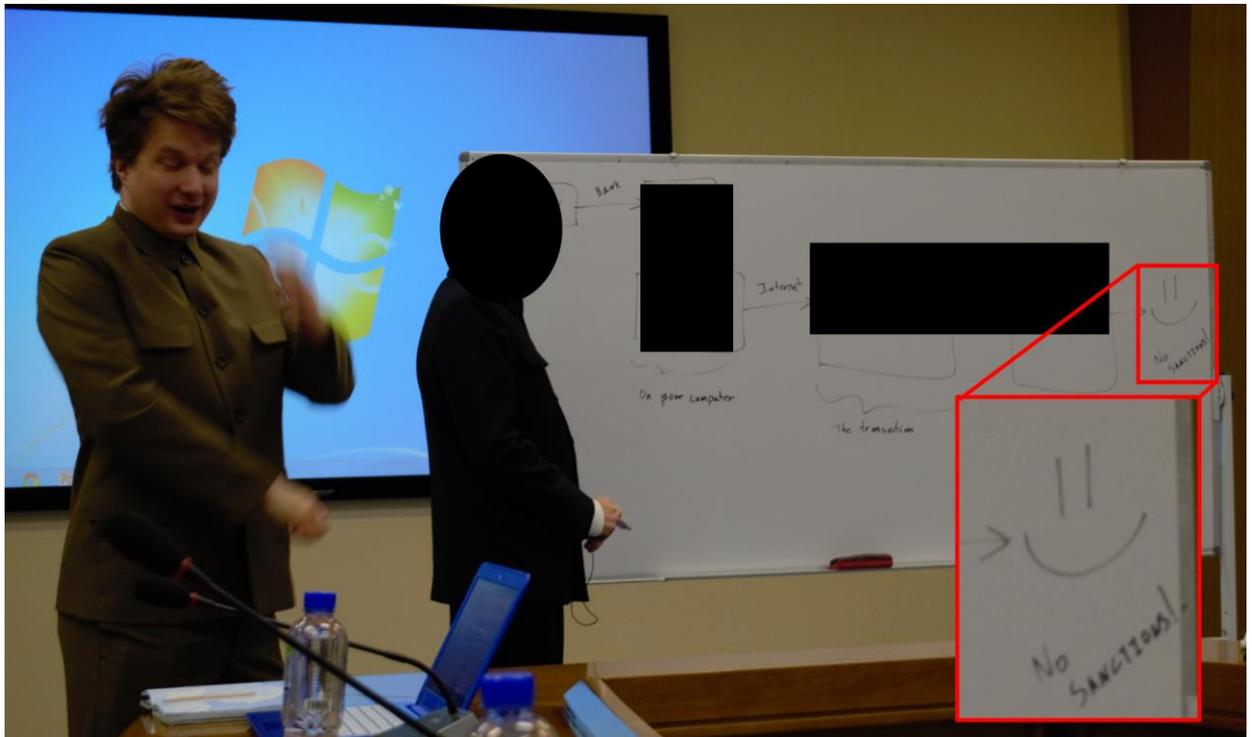
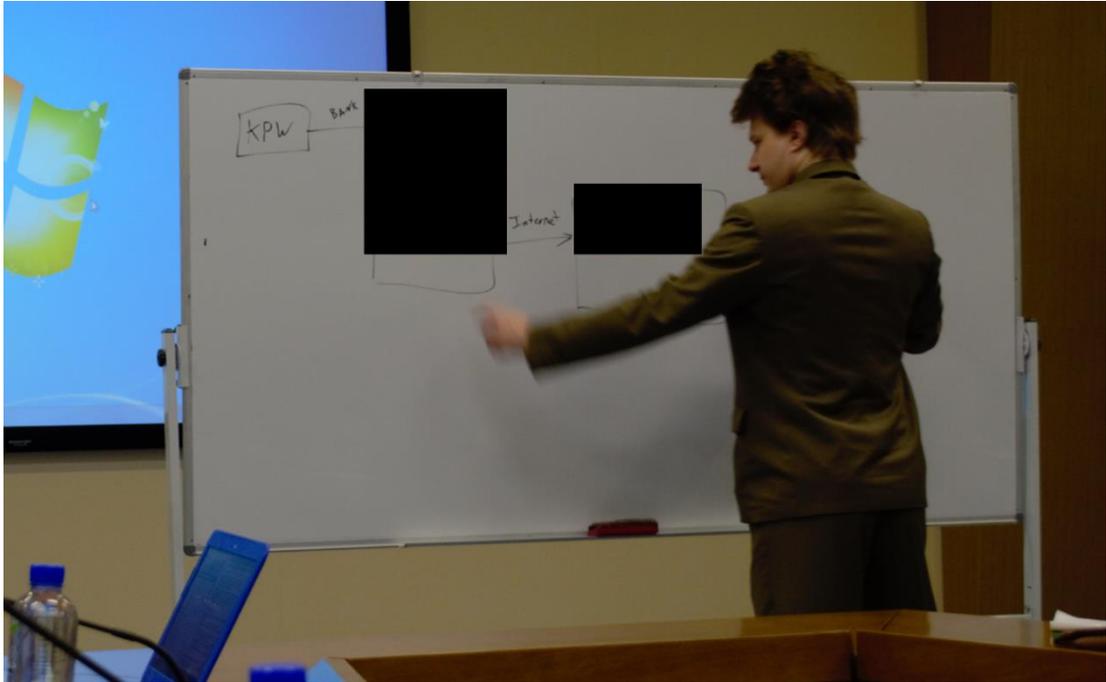
[S]ay things like you know, we want there to be less artillery in the DMZ, and say you know if there is less artillery then that we agree to, I don’t know, say one of the missiles, exactly one being deactivated, or something like that and this is the way to start small, otherwise we get comfortable with technology.

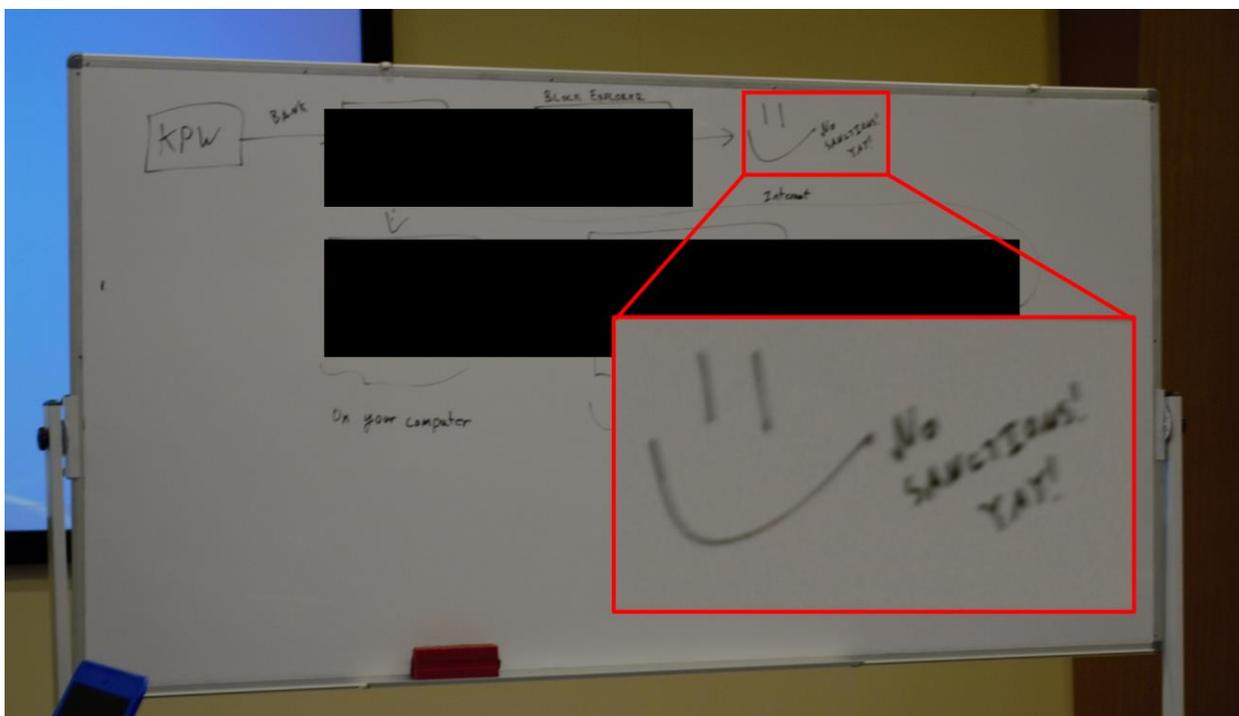
In other words, Griffith specifically pitched the DPRK audience on the idea that they could gain leverage in sanctions negotiations by placing a “module on a missile” to “deactivate” the missile, but only “if you [i.e., the United States] get rid of the sanction, the missile are really gone.” Griffith also pitched the use of the same technology to leverage the DPRK’s control over missiles to negotiate for “less artillery in the DMZ,” that is, weapons in the Korean Peninsula’s Demilitarized Zone.

Based on photographs taken at the Conference, Griffith’s admissions, and information

obtained from a witness who attended the Conference and was prepared to testify at trial, Griffith gave additional presentations, which were not audio-recorded, on the second day of the Conference. During those presentations, Griffith and CC-2 mapped out on a whiteboard how to convert North Korean won into cryptocurrency based on U.S. dollars and to use that cryptocurrency, specifically using the Ethereum network, as a means to evade sanctions. Photographs from the Conference depicted Griffith's illustration of how to send a cryptocurrency transaction using the Ethereum network, ending in his notations of "no sanctions yay" and "no sanctions ☺." This presentation included explanations of what parts of a cryptocurrency transaction could be publicly viewable and what would remain secret, such as the identities of the parties to the transaction. Griffith wore a North Korean uniform while presenting to his audience, as reflected in the images below¹⁶:

¹⁶ The Government has redacted these images to prevent the risk of harm to national security, and added red boxes to make relevant portions more visible in a larger size. The Government respectfully requests to file the original, unaltered versions of these images under seal as Exhibits to this submission, marked GX 208, 215, and 216, to avoid the risk of further harm posed by publicizing the specific sanctions-evasion instructions and techniques described and promoted by Griffith and his co-conspirators.





Griffith also delivered a presentation on theoretical concepts underlying blockchain technology, such as “proof of stake” and “proof of work.” During that presentation, Griffith described a specific cryptocurrency security device that he had been assisting to develop, encouraging Conference attendees to view the product’s website. At one break, a recording captured Griffith commenting to CC-2 that he was puzzled by one of the North Korean’s questions relating to compliance, because, as Griffith rhetorically asked, “are you not aware that, like . . . that everything you do, every transaction . . . is a criminal transaction? This is exactly what we’re doing.” GX 712.

Throughout the Conference, Griffith and CC-2 answered questions from North Korean Conference attendees with the assistance of an interpreter, which focused on the technical aspects of blockchain and cryptocurrencies, and on the ways in which those technologies could be used to evade sanctions. PSR ¶ 40. For instance, one North Korean attendee asked whether the regulation of blockchain and cryptocurrencies would be expected to increase over time. In the audio

recording, CC-2 responds:

The issue with blockchain technology is let's say, a regulator does regulate against something or a government, let's say the US tomorrow says all transactions on cryptocurrency between the DPRK and the rest of the world are banned, the question becomes: how can they ban it? The answer is they can't, because unless they were to gather every single computer on the entire planet, and program each and every single one of these computers that they would not be able to accept cryptocurrency transactions from DPRK, which is impossible, no one could ever do that, then it will always work. As long as there is an Internet connection that the DPRK has, and someone on the other side has, then the transaction can happen. So it is more or less impossible, even if they were to create a law, or to create a sanction, that that sanction would be enforced. They couldn't enforce that sanction. Not like the current system where they just send a letter or maybe Swift and say don't process the transaction. You can't do that with a blockchain because it's hundreds of thousands of millions of individual computers owned by individual people that would be making that transaction happen.

In the course of the Conference, CC-2 explained that SWIFT was “a U.S. company . . . [that] decides where the money can be moved from one country to another through other banks,” and introduced Griffith as “one of the early scientists in Blockchain” who had “anonymously started building a technology that would allow for Swift not to control transactions anymore” and “found a way to get rid of Swift.” CC-2 summarized that “[t]hanks to the great efforts of these scientists, now it is possible to transfer money across any country in the world regardless of what sanctions or any penalties that are put on any country by any other country or by any individual group. . . . In particular relevance to the DPRK, this means that be using this technology, the DPRK can freely move money around the world without the U.S. blocking any of these transactions or stopping other countries or other individuals or other organizations or other governments from receiving the money or sending money to DPRK.” GX 403-A.

The above-excerpted audio recording also demonstrates that the same questioner then

appears to have asked a follow-up question about whether the DPRK could access the exchanges where cryptocurrencies are traded, or whether they had to use “OTC [over the counter] service providers,” which could be difficult due to U.S. sanctions. In response, CC-2 and Griffith made the following statements:

CC-2: That’s a really good question.

Griffith: I like him, he’s really smart.

CC-2: So let me explain to you, so in essence not much difference. The difference between an OTC provider and an exchange is an OTC means that the purchasing is happening off the market. What that means is that, the rest of the market can’t see that you bought that bitcoin. So it’s as if, with Dr. Virgil, he decided to privately sell me his bitcoin, or his USDT [U.S. dollar tether, a cryptocurrency], but we do it agreed between ourselves, we don’t agree it and then everyone in the room knows we did it. We go outside and we have a conversation and we sent it between ourselves. So that tends to be a way in which governments and large entities prefer to do the transaction because [they] don’t want the whole world knowing that they just moved a significant amount of money between each other.

In terms of your question on sanctions, the largest OTC desks in the cryptocurrency space, most of them operate out of China. So most of them, the DPRK obviously has more friendly relations with China than probably any of the other large powers at this current stage, and I personally don’t think that finding an OTC provider in China would be very difficult for DPRK.

Griffith: And if China doesn’t work, Singapore will probably be able to do it.

During another part of the Conference, a Conference attendee asked, in Korean, for a “more clear idea of what is blockchain.” As the audio recording reflects, Griffith responded:

So I was asked what a blockchain is, and so there are several ways of looking at it. The most abstract one is that it is a database where no single person has a back end access where they can get in. So before when there were different databases . . . it lives on one server

somewhere. Where that server is . . . the government could edit . . . and control it. Blockchain is interesting in that the database is split among servers all over the world. So this makes the database slower but it makes it where no single person can control it. That's fundamentally the new idea.

The new idea's having a database that we can all read from and we can all pay a very small amount of money in order to write to it. And anyone can do this.

So the term blockchain—so a block, basically it is a list of updates. Let's say A sends money to B or something like that so this whole block is like a list of a hundred transactions and the chain tells you which order the transaction goes through. So if you have two transactions—say A sends money to B, or A sends money to C, you have to know which ones came first. So the block says what are the transactions and the chain says what order they go in.

Probably the coolest thing about blockchain is that it lets you treat digital data in a new way. So before, let's say you have a movie, you can always copy the movie and give it to your friends. This is not very good for money—you can't really copy money, that doesn't really work anymore. Blockchain is the ability that when you give . . . to someone, you can no longer give it to someone else.

Finally, during another part of the Conference, the audio recording reflects that Griffith made the following statements:

So, a lot of this technology is still very new and most of this paper is about different tradeoffs and you know, how to make it resistant to different kinds of attacks. So if like the U.S. wanted to corrupt the blockchain, what are some ways to make it harder for them to do it? People haven't really decided that's like the best design yet, but the designs are getting better and, yeah, so I guess, starting now would be a way to get in early and achieve dominance.

A Conference attendee then asked whether there exists “any organization or party that manages or takes charge of [Bitcoin's] distributive database system.” Griffith, as reflected in the audio recording, responded:

Yeah, that's an easy question with a hard answer. So there is a group that does upgrades to Bitcoin. But they don't try to control it. So one of the interesting things about blockchain is that if you don't like

how it's being run, you can always copy it and make your own. So there is a current group that does this—they're called Bitcoin Core, and-but you know, they're not part of the U.S. They're just random people all over the world. If you decide that you don't like them, you can just go without them and there's no problem. So in short, there is a group, they do upgrades, but you aren't tied to them—you can go without them if you want.

4. Griffith's Other Activity During the April 2019 Trip to the DPRK

In addition to his attendance and presentation at the Conference, Griffith used his trip to advance his plan to provide cryptocurrency services to the DPRK and develop cryptocurrency infrastructure within North Korea. PSR ¶ 42.

On April 20, 2019, Griffith called CC-5, a cryptocurrency colleague, from his Facebook account while still in the DPRK, and placed CC-5 on the phone with CC-6, his DPRK government "minder." Griffith then wrote to CC-5 on Facebook asking her to "send us the Korean language materials." EF_SDNY_0001168. Griffith's personal notes from the same day(reflect that in North Korea, Griffith "[s]hot USSR Pistol and Sniper Rifle used to kill Americans." GX 804. Griffith's personal notes from his time in the DPRK also reflect his observations that the North Koreans were "very proud of their capture of US military craft," reference a "[v]ideogame where you shot American Tanks," and state that he "would like to get a copy of the video from the Liberation museum saying how America started the Korean war." GX 803. Griffith circulated a link in a chat conversation among attendees of the Conference relating to the U.S.S. Pueblo, a U.S. Navy ship attacked and captured by North Korea in 1968, and now used by the North Koreans as a museum. The U.S. servicemembers aboard the U.S.S. Pueblo were held hostage for nearly a year. Griffith toured the ship while in North Korea.

While in North Korea, Griffith made plans with CC-2 and other Conference attendees to renew Griffith's plan to establish a cryptocurrency mining node in the DPRK. PSR ¶ 26. Griffith

also proposed plans, along with CC-2 and other Conference attendees, regarding ways for the DPRK to make money by selling its domain name. Griffith planned to return, bringing cryptocurrency equipment like hardware wallets with him.

On April 22, 2019, while still in the DPRK, Griffith exchanged the following additional electronic messages with Individual-1:

Griffith: Dprk is interested in oracles
For their sanctions negotiations.
E.g., whether the sanctions have been lifted
Could be high visibility work

Individual-1: How do you even make an oracle for that?
Augur?

Griffith: Not a crazy idea
Newspapers? The UN?
They are into any oracles relevant to negotiations

Individual-1: Newspapers and the UN don't cryptographically sign
things in standardized formats, do they?

Griffith: We could talk the UN into doing it I bet
Rhombus.network can do it for the newspapers

EF_SDNY_0001170. Griffith appears to have used the term "oracle" here to refer to a kind of mathematical "smart contract" that could be constructed for the DPRK, potentially using a computer software platform known as Augur which is built on the Ethereum blockchain. Constructing a smart contract on the Ethereum blockchain requires the use of ether, its cryptocurrency coin.

Two days later, on April 24, 2019, while still in the DPRK, Griffith messaged Individual-1 with an additional business proposal, stating "DPRK wants to make foreign journalists put a deposit on Augur that is forfeited if they write a highly unflattering article." Griffith noted further that he "got along very well" with his DPRK government minder, and that the minder was "going

to try to get Blockchain.kp for us. For the dprk Blockchain association.” Griffith’s message to Individual-1 aligned with a “to do” list Griffith maintained during the Conference as “Notes for the group,” which included plans to “[a]ttempt to acquire” two DPRK-based Internet domains relating to cryptocurrency – “blockchain.kp” and “crypto.kp.” GX 810. In the same notes, Griffith wrote: “I suggest we do a special 1-hour session Q&A for expert topics.” *Id.* Griffith’s contemporaneous notes from the Conference also reflect his view that the “DPRK probably has some assets to auction off,” including “IP [Internet Protocol] space,” “domain names,” “webhosting,” and potentially “phone numbers,” corroborating his interest in the value of Internet domains from the DPRK. GX 802.

Griffith’s emails immediately following the Conference also reflect that he was continuing to engage North Koreans about his plans to build cryptocurrency infrastructure. For example, Griffith wrote to CC-5, “I know my North Korean guide gave a [thumbs up emoji] to the idea of sending 1ETH¹⁷ forward and back,” that is, demonstrating how a cryptocurrency transaction could be conducted from within the DPRK, bypassing U.S. and U.N. sanctions. GX 3061. On April 25, 2019, in a social media chat with a friend, Griffith wrote that the North Koreans “are interested in using crypto to get around sanctions[,] But there’s no active program to do so.” GX 2413. When the friend asked Griffith if the DPRK had sufficient capability to do this, Griffith responded, “They do. But not for a wide deployment.” *Id.* The friend noted, “Ok maybe that’s why they are inviting people to give tasks,” to which Griffith responded, “That sounds correct.” Griffith then asked the friend, “Want to go? I could get you an invite.” *Id.*

Griffith also attempted to recruit other cryptocurrency professionals to travel to the DPRK

¹⁷ ETH is the symbol for ether, the unit of cryptocurrency created by the Ethereum Foundation.

in order to provide similar services to the DPRK, at the behest of the DPRK government. *See* GX 2416. Within just one day of leaving the DPRK, Griffith posted on Facebook to recruit professionals to travel to the DPRK “to give lectures on science/technology,” representing that the North Koreans “have reached out to me [] for recommendations of new people to invite to their country” and specifying that he was recruiting for experts in “computer science, agriculture, or blockchain.” GX 2601. Numerous contacts expressed grave concerns about Griffith’s proposal, which he ignored, describing North Korea as “one of the most murderous authoritarian states in the world,” and citing that North Korea “uses crypto currency to smuggle sex slaves and heroin in large numbers and engages in significant Bitcoin blackmail and hacking schemes.” *See* <https://www.facebook.com/virgil.gr/posts/10112756681859159> (Griffith’s complete Facebook post and comments). The same day, April 26, 2019, Griffith wrote to a contact that “I’ve [been] able to suggest that they invite other people. Would you like to go? You’d have to give some lectures on Blockchain/crypto.” GX 3054. The next day, on April 27, 2019, Griffith emailed CC-6, his DPRK government handler, identifying a computer scientist and stating, “He’s interested in teaching computer programming and machine learning”; Griffith further reported that “I’ve asked a few of my researcher friends if they’d like to visit DPRK,” and inquired if a stay for “longer instruction (say ~ 1 month)” and funding for their accommodations would be possible. GX 3055. Griffith emailed CC-6 again that day, stating:

I’ll be sending you two PhD scientists who are interested in visiting and lecturing in DPRK Here’s what the DPRK would need to [do] for journalists to put deposits to get access to the country: <https://kleros.io>. It looks like a better solution than Augur.¹⁸ If you

¹⁸ Both Kleros and Augur, as described in part above, are platforms that offer smart-contract services built on the Ethereum blockchain. The link provided by Griffith – <https://kleros.io/> – describes Kleros as “a decentralized arbitration service.”

decide this is something you want to pursue, I'll ask some colleagues in Singapore about developing it. If the DPRK can pay for it, great. But if not, the Singapore contractor can just take a percentage from the pot of journalists using the platform.

GX 3056. Griffith reported to one of these proposed scientists that the North Koreans had rejected that scientist because his expertise was “not [] related to DPRK’s main missions,” or in other words, he was not useful to the DPRK’s core missions, unlike Griffith. GX 2414.

Griffith also engaged CC-1 to further his plans, writing to CC-1 on May 14, 2019, “there is talk of doing a *joint blockchain conference* between Pyongyang and Seoul. The DPRK seemed to express a lot of interest in doing this . . . but I haven’t heard from them since I left DPRK.” GX 3059. Griffith also represented that he had identified several people to bring to the DPRK and that he was “compiling a list” for CC-1. *Id.* On May 16, 2019, CC-1 wrote to Griffith, stating that “the situation is still serious (Max Thunder military exercises)¹⁹ and such event is not possible for now,” noting that “[t]he blockchain conference you attended required the maximum level of authority in our [the DPRK] government.” GX 3061.

Shortly after leaving the DPRK, on April 26, 2019, Griffith also wrote to his parents and sister:

Griffith: I think I’m going to be the connector in Blockchain-mediated economic relations between dprk and South Korea

Griffith: Should be fun

Griffith: Hopefully won’t have much jail time for it

¹⁹ The “Max Thunder” military exercises are joint training exercises conducted annually by the United States and South Korean air forces, which are regarded by the DPRK as a “military provocation” justifying their own threats of a “nuclear showdown.” *See, e.g.,* <https://www.cnn.com/2018/05/25/asia/us-south-korea-max-thunder-drills-intl/index.html>.

Griffith: I'll try to be wealthy enough to pay my bail.

GX 1307.

The same day, CC-1 wrote to the Encrypted Group Chat that he would be conducting interviews with “blockchain press” and requested a photograph of the group from the Conference, but noted that he didn’t want to “expose” anyone for having attended. Griffith replied, saying “No group photos of me please.” GX 202. When a Conference attendee circulated a photograph of CC-2 in front of a whiteboard on which CC-2 had written, among other things, “OTC Exchange,” referring to the over-the-counter exchange of cryptocurrency for fiat currency, CC-2 responded, “Guys don’t publish the last one [a]s it has info on it on Otc.” *Id.* CC-2 also wrote to the group: “Hi all I just got pulled by police at the airport[.] Would recommend removing any photos of conference as they knew a lot.” *Id.* Griffith subsequently deleted his Telegram account from the Encrypted Group Chat.

5. Griffith’s Statements to Law Enforcement after the Conference

After the Conference, Griffith was interviewed at the U.S. Embassy in Singapore and agreed to meet with the FBI. Search warrant returns for Griffith’s social media accounts reflect that on May 21, 2019, Griffith informed a friend in a Facebook chat that “[t]he FBI wants to talk to me about North Korea,” and stated that he intended to meet with the FBI because “I’ve already technically violated the law[.] And violated sanctions.” GX 2417. FBI agents interviewed Griffith in person on May 22, 2019 and November 12, 2019. The FBI also interviewed Griffith over the phone on November 6, 2019.

During these interviews, Griffith acknowledged that he traveled to the DPRK to attend the Conference as the keynote speaker. He acknowledged that he knew it was illegal for U.S. citizens to travel to the DPRK, and that the State Department denied his request for permission to travel to

the DPRK. Griffith told the agents that he corresponded with officials at the DPRK Mission in Manhattan to facilitate his travel, and that he sent the requested documents for travel to the DPRK Mission's email address. Griffith also stated that he paid the Conference organizer 3,000 to 3,500 Euros to attend the Conference, and that he believed some of that money might have been provided to the DPRK government.

Griffith stated that, prior to the Conference, he received approximately 15 PDF files of technical papers, which he believed CC-2 had provided to the DPRK government, and which the DPRK government had approved for the Conference. CC-2 told Griffith to create his presentation for the Conference using this "approved content." In preparation for his remarks, Griffith developed a PowerPoint presentation that was based on these approved PDFs. According to Griffith, CC-2 told Griffith to stress in his remarks that cryptocurrency and blockchain technologies could be used for "money laundering" and "sanctions evasion," since that was the basis for the attendees' interest in those technologies.

Griffith also described the Conference to the interviewing agents. Griffith stated that the Conference had approximately 100 attendees, only some of whom appeared to understand cryptocurrency and blockchain technology. Griffith also described three young men who sat in the back and asked more technical and specific questions, including questions that addressed complex topics, such as "proof of work" versus "proof of stake" in the mining of cryptocurrencies. As to Griffith's keynote address, Griffith reported that there were technical difficulties, so Griffith discussed the topics in his PowerPoint presentation verbally and used a whiteboard to draw diagrams during his discussion.

Griffith acknowledged to the agents that the PDFs were like a course textbook, and that Griffith was the lecturer who explained the content to the audience like a teacher. He assessed that

he may have introduced new concepts to the North Korean Conference attendees, and that the attendees left with a better understanding of blockchain and cryptocurrency technologies. Griffith also noted that a major selling point to the North Koreans at the Conference was that cryptocurrency could make the DPRK independent from the international banking system. Griffith also told FBI that the DPRK could not build a cryptocurrency without China's assistance, but that the Conference provided "bottom-up interest in cryptocurrency."

During Griffith's second interview with the FBI, on November 12, 2019, Griffith described in greater detail how CC-2 planned to enable the transfer of cryptocurrency, on behalf of the DPRK, from the DPRK to China. According to Griffith, CC-2 drew a diagram for the Conference attendees to demonstrate these steps. Griffith described that at the first step in the process, the DPRK central bank would perform a one-for-one swap of a cryptocurrency coin and fiat currency such as the North Korean won. Next, the cryptocurrency would be digitally placed into a wallet. From that point, it would then be transferred into U.S. dollar, euro, or Chinese renminbi. As set forth above, evidence from the Conference captures CC-2 and Griffith speaking together to Conference attendees regarding OTC exchanges of cryptocurrency. Photographs from the Conference demonstrate that Griffith worked together with CC-2 to instruct the DPRK audience on these financial transaction steps for the purpose of evading sanctions.

During the first interview, on May 22, 2019, Griffith also informed the agents of his desire to return to the DPRK, and to facilitate cryptocurrency exchanges with the DPRK. PSR ¶¶ 45, 46. The agents advised Griffith that doing so would likely violate U.S. law, including the prohibitions associated with IEEPA.

6. Griffith Continues to Pursue the Advancement of DPRK Cryptocurrency Services

Despite the admonishment from FBI, Griffith continued to pursue providing additional

services to the DPRK. PSR ¶ 49. For instance, on August 4, 2019, Griffith wrote CC-2, “I’d like to do the sending of the 1 ETH between Pyongyang and Seoul. And it seems the only way to get that to happen is for us to take another trip to DPRK.” PSR ¶ 49. In response, CC-2 asked, on August 5, 2019, if Ethereum would “sponsor the next conference and we do a whole thing around sending 1 ETH?” On August 6, 2019, Griffith conveyed that while his company might not be willing to transact in and for the DPRK, he was eager to do so, writing, “Ethereum Foundation can’t touch anything DPRK. B[ut] I can fund some things myself. I can also get the South Korean buy-in for the sending of 1 ETH.”

Also on August 6, 2019, Griffith wrote to a U.S.-based friend (“Individual-5”):

Griffith: I want to go back to North Korea.

Individual-5: Why? What do you hope to gain from your second visit?

Griffith: I need to send 1 [ether] between North and South Korea.

Individual-5: Isn’t that violating sanctions?

Griffith: It is. That’s why I’m going to get a South Korean to do it.

Individual-5: What [South Korean] would dare to take that risk?

Griffith: I’d do it

Individual-5: You aren’t South Korean.

Griffith: Just need to find a South Korean Virgil.

Individual-5: oh lol

Griffith: There’s got to be at least one who wants to make a name . . .

Individual-5: Would it damage the reputation of Ethereum?

Griffith: I predict it will be a net positive

Individual-5: It makes me nervous for you to defy the government and go again

Griffith: I'll figure something out . . . Worst comes to worst I'll send an emissary.

GX 1105.

The next day, on August 7, 2019, Griffith sent audio messages to Individual-5, in which Griffith stated: "I'm aware this is a high stakes game, but I feel like I'm a pretty competent player of the game Probably worst comes to worst, I'll find someone to send as like an emissary to go and I'll like tell that person what to do via the phone. Yeah, I can always do that, because it seems like the Americans let you get away with it once." GX 1107A, 1107B.

Griffith proceeded to identify a South Korean national, Individual-6, and to proceed with plans to use Individual-6 as his emissary for the transaction, which he had repeatedly made clear he understood would violate the sanctions regime. On August 28, 2019, Griffith engaged in the following social media chat with Individual-6:

Individual-6: if I can make this happen, can the ether be sent from my wallet app?
if they say its not illegal

Griffith: Sure
It's most definitely illegal
It violates UN sanctions

Individual-6: LOL

Griffith: But they probably won't do anything about it

GX 2421. Individual-6 ultimately declined to conduct the transaction for Griffith.

On September 9, 2019, Griffith sent separate emails to a cryptocurrency business executive and an individual working at an American research center with a link advertising another DPRK

cryptocurrency conference planned for 2020—nkcryptocon.com. On October 28, 2019, a representative of an international technology association emailed Griffith referencing the DPRK’s internet domain (“.KP”), requesting that Griffith “[p]lease advise our Korean friends” of how to register for a meeting planned for Australia, and proposing that Griffith “put me in direct contact with [CC-1].” GX 3078. Griffith forwarded the email to CC-1, stating that this was “an invitation for a delegation from DPRK” to an event and offering to “crowdfund the delegations’ tickets.” *Id.* Griffith further noted that he was “shilling,” or promoting, “your nkcryptocon.com,” that is, the 2020 DPRK cryptocurrency conference planned by CC-1, CC-2, Griffith, and others, which ultimately did not occur. *Id.*

On September 20, 2019, in a social media chat with Individual-6, Griffith discussed a *CoinDesk* article stating that “North Korea is working on building its own cryptocurrency to get around the tough international sanctions.” GX 2422. The article stated that “the new crypto may be pegged to an asset within North Korea” and quoted CC-1, who was described as “the official managing North Korea’s cryptocurrency conferences and a special delegate for the nation’s Committee for Cultural Relations,” as stating that “we are in the phase of studying the goods that will give value to it,” that is, the cryptocurrency coin. Griffith commented that the article “[s]ounds right,” and stated that “[i]t’s exactly the kind of thing they would want[,] [c]ontrolled digital money.” *Id.* When Individual-6 stated that he “thought they were scared of [the] internet’s openness,” Griffith replied, “Yeah, it’ll just be within their intranet,” referring to North Korea’s tightly controlled internal computer network. *Id.* On October 2, 2019, in a text exchange with family members, Griffith noted that he might be fired from Ethereum and stated that, if he was, he might instead “setup a money laundering company in North Korea.” GX 1310.

Immediately after his first FBI interview in May 2019, Individual-5 also advised Griffith, via WhatsApp on May 23, 2019, that he should get his “taxes in order” because he was dealing with the FBI, and “[t]hey might look for ways to get you and taxes is a common pitfall.” GX 1103. Griffith responded, “They have plenty to get me with. Without any taxes. Visiting dprk they can take away your passport. And imprison for 10 years.” *Id.* In November 2019, the defendant admitted to an employee of another cryptocurrency company, “I discovered I didn’t file a tax return for years 2015-2018. But weirdly the IRS hasn’t contacted me about it. I’m considering just filin[g] my taxes in 2019 and just pretend I had no one in 2015-2018. I know that’s illegal, but i was basically a student in 2015-2017 doing postdocs I had <100k income on those years.” Dkt. 131 at 23 (Gov’t Mot. in Limine).

Also during the period after his first interview with the FBI, the defendant explored the possibility of renouncing his United States citizenship with at least three individuals, including his father. For example, Griffith communicated with several individuals about his plan to purchase citizenship from St. Kitts, telling one person he was “working on it.” Within five days after the defendant’s November 2019 meeting with the FBI, he told Individual-3 via email about the FBI meeting and stated, “I want to get a second passport asap. I didn’t like having my back against the wall I can get a passport from St. Kitts for 100k USD. And that you can just buy and get it within a month or so.” *Id.* at 23-24.

At the time of his arrest, months after the Conference, Griffith was carrying three North Korean texts by Kim Jong-Il and Kim Jong-Un in his suitcase: “Kim Jong Il: On the Juche Idea,” “Kim Jong Un: On Accelerating the Victorious Advance of Socialism,” and “Kim Jong Un Aphorisms,” and a cryptocurrency hardware wallet. *See* GX 102A, 103A. When his cellphone was seized, he asked to power it off, in an apparent attempt to make it more difficult for law

enforcement to search it.

C. Griffith's Guilty Plea

On September 27, 2021, the morning of trial, the defendant pleaded guilty to the charge contained in the Indictment: conspiring to violate IEEPA both by illegally providing services to the DPRK and by evading and avoiding the requirements of U.S. law with respect to the provision of services to the DPRK, from at least August 2018 through November 2019. PSR ¶ 4. At the time of the defendant's plea, jurors had been summoned for service in connection with the case and witnesses had traveled internationally in order to appear for trial, including at least one U.S. Government employee who appeared in response to a defense subpoena. The defendant pled pursuant to a plea agreement, which set forth a stipulated Guidelines range of 63 to 78 months' imprisonment (the "Stipulated Guidelines Range"). PSR ¶ 4(C)(1). The parties agreed that the defendant was in Criminal History Category I and that the applicable offense level was 26. PSR ¶ 4(A)(4), 4(B)(2). The offense level reflected that the offense involved the evasion of national security controls and financial transactions with a country supporting international terrorism, and that the defendant had used a special skill to commit the offense, namely, his cryptocurrency expertise. In addition, the parties agreed that the applicable fine range was \$25,000 to \$1,000,000. PSR ¶ 4(C)(1).

D. The Presentence Report and Defense Submission

In the PSR, Probation calculates the same offense level, Criminal History Category, and Guidelines range of 63 to 78 months' imprisonment reflected in the plea agreement. PSR ¶ 102. Probation recommends a Guidelines sentence of 63 months' imprisonment and fine of \$25,000. PSR at 33. Probation notes that "Griffith's involvement in the instant offense jeopardized the national security of the United States by undermining the sanctions that the President and Congress

had enacted,” and that his own email communications “indicate that Griffith was fully aware of his actions and that he would be breaking the law, but he persisted anyway.” PSR at 34.

The defendant seeks a downward variance of 24 months, citing his personal characteristics, his alleged efforts to cooperate with law enforcement, his own view that deterrence is not needed, and his own characterization of the offense as “less serious” than others.

For the reasons set forth below, the significant variance sought by the defendant is not warranted in this case and would fail to meet the legitimate aims of sentencing. The Court should impose a sentence within the Stipulated Guidelines Range, which is the sentence warranted by Griffith’s extended, brazen, and relentless efforts to evade U.S. sanctions on North Korea.

DISCUSSION

I. Applicable Law

“[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, a sentencing judge must consider the 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 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 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).

II. A Guidelines Incarceratory Sentence and Fine Are Warranted

A significant incarceratory sentence within the Stipulated Guidelines Range is necessary to reflect the nature and seriousness of the offense, to promote respect for the law, and to provide needed deterrence both to Griffith and to others. Griffith was a leader in the cryptocurrency industry, who chose to provide his services to a sanctioned state sponsor of terrorism that threatens U.S. national security and even the security of its own citizens. Griffith provided instruction for sanctions evasion and money laundering through cryptocurrency, among other things. His conduct was not a matter of a momentary indiscretion. Griffith engaged in a prolonged plan to find ways to do business with North Korea, which continued even after he was admonished by law enforcement not to travel to North Korea, and again, after he returned, when he was admonished to stop violating sanctions. He did so brazenly, repeatedly reaffirming that he knew what he was doing was wrong. Though he considered the criminal nature of his actions, Griffith was undeterred precisely because he expected that he could rely on his privileged stature to avoid any serious consequences for his crime. A substantial Guidelines sentence is needed to address this incredibly serious offense, to promote respect for our sanctions regime as a cornerstone of U.S. national security, and to deter future violations of U.S. sanctions by showing they will be enforced. In addition, a fine towards the upper end of the Guidelines range – \$1,000,000 – should be imposed to fulfill the same legitimate purposes of sentencing.

A. The Seriousness of the Offense and Need to Promote Respect for the Law

Griffith's crime served to undermine U.S. sanctions laws that were part of a broad international effort directly related to a variety of the DPRK's dangerous and deadly policies and actions, including its military nuclear program, its ballistic missiles program, its sponsorship of terrorist organizations, and its rampant human rights violations. The gravity of the threat posed by the DPRK to the United States and its allies was known to Griffith, as he repeatedly made clear in his communications with co-conspirators and others. *See, e.g.*, PSR ¶ 29 (Griffith acknowledging that DPRK would "probably like to start" "funding their drug trade and nuclear program with crypto"); *supra at 20* (Griffith describing to DPRK audience how to use blockchain to "put a module on a missile"); GX 803 (Griffith's personal notes reflecting that he "[s]hot USSR Pistol and Sniper Rifle used to kill Americans."). And Griffith was well aware that his provision of cryptocurrency services, in violation of U.S. sanctions, risked aiding the DPRK in precisely those hostile and dangerous endeavors that the sanctions were intended to deter. In his own words, Griffith stood to deliver "Blockchain talent that'll let [the DPRK] get around sanctions." PSR ¶ 29. Indeed, throughout the conspiracy, Griffith demonstrated time and time again that he was fully aware of the sanctions, that he knew he was violating them, that he knew he was helping North Korea to evade them, and that this would not stop him in pursuing the criminal venture. *See, e.g.*, GX 2417 (Griffith acknowledging in a private message "I've already technically violated the law[.] And violated sanctions"). A substantial sentence within the Stipulated Guidelines Range is necessary to reflect the seriousness of this offense, to promote respect for the law – which Griffith made clear he utterly lacks – and to provide just punishment. *See* 18 U.S.C. § 3553(a)(2)(A)-(B).

As described above, the United States and international sanctions regime was developed to combat the DPRK government's sponsorship of terrorism, human rights abuses, rogue nuclear program, and rampant oppression and illicit conduct. Griffith showed no regard for this national

security effort, as he jumped at the opportunity to advance his own personal business interests in service of the DPRK, while betraying the interests of his own country and the international community in the process. Griffith's statements reflect that he believed the DPRK would like to "start" "funding their drug trade and nuclear program with crypto," and acknowledged but disregarded warnings from others that the DPRK was engaged in widespread human rights abuses including maintaining "concentration camps."²⁰ Despite this knowledge, Griffith worked to serve the DPRK regime over an extended period.

Yet, in his sentencing submission, Griffith seeks to undermine the gravity of his offense, downplaying it as "less serious," consisting of merely sharing "high-level general information," and falling towards "the lower end of the universe of sanctions offenses." Def. Mem. at 27-28. This is a disturbing minimization of the defendant's years-long, willful, and unabashed effort to evade and subvert U.S. sanctions that were part of an intensive effort by the United States, and the global community of the United Nations, to curb the nuclear ambitions of a state sponsor of terrorism and a leading threat to world peace and stability.

The defense inaccurately claims that while Griffith presented proposals for the "potential uses" of cryptocurrency and blockchain technology by the DPRK, for the express purpose of sanctions evasion, he did not actually help implement his plans. *See* Def. Mem. at 26. This claim is belied by the evidence. Prior to the Conference, Griffith worked to establish a cryptocurrency mining node in North Korea for months, proposing to pay thousands of dollars of his personal funds to accomplish the goal, including a "consulting fee" to an intermediary and a purchase of

²⁰ For example, in an August 12, 2019 chat conversation obtained from Griffith's cellphone, a friend argued with Griffith about his travel to North Korea and asked Griffith: "Did you get to choose to see the concentration camps North Koreans are involuntarily sent to or was that not on the route?" Griffith responded that "They [the North Koreans] acknowledged that the camps do exist."

the “mining rig” equipment, to “setup a dprk shell company,” and to “funnel[] things through Singapore/China” to dodge U.S. sanctions, among other things. Griffith marketed the plan by highlighting that “[a]nother benefit of an Ethereum node in dprk” would be to “make it possible for them to avoid sanctions on money transfer” and “help them circumvent the current sanctions on them.” During the Conference, Griffith corresponded with Individual-1 about specific proposals to design blockchain services for the DPRK and to obtain hardware wallets for them at their request. Days after returning home from the DPRK, Griffith emailed his DPRK government handler, not only offering to send more “PhD scientists” to the DPRK to provide instruction, but also telling him that “[h]ere’s what the DPRK would need to [do] for journalists to put deposits to get access to the country.” And Griffith contacted an array of experts in an effort to recruit them to join him in assisting the DPRK. Griffith also provided a direct link to a service to build such a mechanism, and proposed to “ask some colleagues in Singapore about developing it” for the DPRK, either in exchange for payment or a percentage of proceeds. It does not matter that Griffith did not “tell [the North Koreans] how anyone actually programs a smart contract,” Def. Mem. at 26, because, as this email shows, Griffith offered up his network of sophisticated contacts to build such bespoke smart contracts for the DPRK as an additional service – and this was among numerous steps Griffith took during the course of the conspiracy to bring to fruition his plan to provide cryptocurrency-related services to the DPRK.

Griffith similarly planned to return to the DRPK with cryptocurrency equipment, including portable hardware wallets, which would empower the DPRK to use cryptocurrency to circumvent the sanctions imposed through traditional banking systems. Even after the FBI admonished Griffith to stop providing services to the DPRK, he persisted, recruiting others to provide services to the DPRK and pressing forward with plans to conduct a second “conference” in North Korea complete

with a live exchange of cryptocurrency – to prove it could not be stopped by sanctions. Once more, it does not matter that Griffith did not “set[] up an entire blockchain” for the North Koreans, Def. Mem. at 26, because Griffith’s presentation showed how all of these sanctions-evading techniques could be performed on the existing Ethereum network. Even CC-2’s proposal for the DPRK to create its own cryptocurrency coin could be done on the Ethereum network, which is built to host initial coin offerings (ICOs) as one of its services.²¹

Griffith nonetheless also claims that, despite willfully violating the law, his actions were somehow driven by subjective good intentions. Def. Mem. 34. First, the evidence discussed above utterly belies that claim, as it shows Griffith bent on advancing his own business and cryptocurrency exploits at any cost, including subverting U.S. sanctions. Moreover, Griffith fails to confront the reality that he presented his claimed “good intentions” to the State Department when he sought permission to travel to the DPRK and present at the Conference, and his request to travel was roundly rejected. He asserted then that cryptocurrency would be a “chink in the armor” of the Kim regime and argued that his trip would somehow be in the interest of the United States. His application was denied. The U.S. Government warned him not to go. Griffith went forward in the face of that express denial, and his claim that he was purportedly acting to further the greater good is easily rejected.

Griffith deeply understood, and brazenly disregarded, the dangers of his conduct. On April 27, 2019, Griffith circulated a link to CC-1, CC-2, and the other foreign participants in the Conference containing an April 2019 paper from a United Kingdom-based think-tank entitled

²¹ See, e.g., “Ethereum and the ICO Boom,” Cryptopedia (2022), *available at* <https://www.gemini.com/cryptopedia/initial-coin-offering-explained-ethereum-ico#section-ic-os-receive-increased-regulatory-scrutiny> (last visited []) (explaining that “the majority of ICOs have taken place via the Ethereum network” which has “contributed to an exponential increase in ETH’s price” and an “ICO boom”)

“Closing the Crypto Gap: Guidance for Countering North Korean Cryptocurrency Activity in Southeast Asia.” GX 202; GX 2613. The paper’s opening lines warned:

Despite recent diplomatic progress with the US, North Korea remains the world’s most significant weapons of mass destruction (WMD) proliferation threat. North Korea has gone to extremes to raise funds and evade international sanctions, recently expanding these efforts to include the exploitation of cryptocurrencies such as Bitcoin. Cryptocurrencies likely play only a peripheral role in North Korea’s overall fundraising and sanctions-evasion activity. However, the sophistication of North Korea’s broader cybercrime operations and its general demand for ongoing financial resources present the risk that its cryptocurrency activity could become a sustained security challenge, particularly as international sanctions lead North Korea to seek financial lifelines outside the mainstream sector. The UN Security Council’s Panel of Experts on North Korea has suggested that cryptocurrencies offer North Korea ‘more ways to evade sanctions given that they are harder to trace, can be laundered many times and are independent from government regulation.’

The paper then identified a series of ways that North Korea could seek to use cryptocurrency to finance its proliferation of weapons of mass destruction. *Id.* Griffith committed his crime knowing full well the potential for his actions to have dire consequences.

The reality is that Griffith’s conduct presented a grave risk to the integrity of the sanctions regime and U.S. national security, and he knew that. The U.N. Panel of Experts specifically assessed that “an objective of the 2019 cryptocurrency conference [in which Griffith participated] was to introduce foreign attendees to trading companies for the purpose of establishing joint ventures or cooperative entities” that would generate money for North Korea. United Nations Security Council, *Report of the Panel of Experts established pursuant to resolution 1874 (2009)*, 195 (28 August 2020) (hereinafter “Panel of Experts Report”), at 196, *available at* <https://undocs.org/S/2020/840>. Following the Conference, the DPRK “reaffirmed its commitment to retaining and developing its nuclear and ballistic missile programmes, in violation of Security Council resolutions,” *id.* at 4, and “exploited” “vulnerabilities within the global financial system

to sanctions evasion activity,” including cryptocurrency providers with a “lack of regulation” and “lack of transparency,” *id.* at 44. Following Griffith’s plea, the U.S. Treasury Department’s 2021 Sanctions Review publicly cited cryptocurrency and related technologies as emerging risks that would “potentially reduce the efficacy of American Sanctions” because they “offer malign actors opportunities to hold and transfer funds outside the traditional dollar-based financial system” and “empower our adversaries seeking to build new financial and payments systems intended to diminish the dollar’s global role.”²² Griffith’s presentations, captured on recordings and in photographs, offered precisely this kind of sanctions-evading instruction and consultation services to his North Korean audience.

B. The Need for Deterrence

A Guidelines sentence is essential to deter Griffith from future crimes, and to deter others from engaging in sanctions evasion. *See* 18 U.S.C. § 3553(a)(2)(B). Griffith acted to shamelessly violate the law, openly betting on the likelihood that he would receive leniency later. That corrupt spirit merits deterrence both for Griffith and for similarly situated others. The history of lenient sentences in sanctions case – which Griffith now seeks to use to his advantage – arguably contributed to that narrative and shows how, for sophisticated actors like Griffith, there has been a failure of deterrence for this crime. That course needs correction.

For Griffith, a highly educated and privileged individual, his expectation that he could minimize the consequences of his actions factored into his choice to break the law. Lenient

²² *Treasury 2021 Sanctions Review* (October 2021) at 2, available at <https://home.treasury.gov/system/files/136/Treasury-2021-sanctions-review.pdf> (last visited Nov. 2, 2021); *The New York Times*, “Treasury Warns That Digital Currencies Could Weaken U.S. Sanctions,” Oct. 18, 2021, available at <https://www.nytimes.com/2021/10/18/us/politics/sanctions-cryptocurrency-treasury.html> (last visited Nov. 2, 2021).

treatment was part of his calculus. For example, shortly after leaving the DPRK, on April 26, 2019, Griffith wrote to his parents and sister that he was “going to be the connector in Blockchain-mediated economic relations between dprk and South Korea,” noting that he “[h]opefully won’t have much jail time for it,” and “I’ll try to be wealthy enough to pay my bail.” GX 1307. On August 7, 2019, Griffith told Individual-5 he recognized it was a “high stakes game” but that he was a “competent player of the game.” GX 1107A. He further noted that since the FBI had admonished him not to return to North Korea, he would find “an emissary to go and I’ll like tell that person what to do via the phone,” rationalizing that he could use a co-conspirator as his proxy because “[y]eah, I can always do that, because *it seems like the Americans let you get away with it once.*” GX 1107B. (emphasis added). Griffith indeed attempted to coordinate to send Individual-6 to act on these plans, telling Individual-6 that the proposed conduct was “most definitely illegal,” “[b]ut they [law enforcement] probably won’t do anything about it.” *See* GX 2421. This evidence shows that Griffith willfully violated the law, but expected to receive little punishment. A significant incarceratory sentence, within the Guidelines range, is necessary to counter Griffith’s flippant belief that he could break the law with impunity.

Griffith tries to argue that specific deterrence is not needed because he has suffered enough from “public humiliation” and a “career in tatters,” but this is far from the reality. Def. Mem. 41. For several years, up to the brink of trial, Griffith turned his criminal case into a cause celebre. Ethereum Foundation founder Vitalik Buterin, one of the most powerful individuals in the industry, has publicly campaigned for him and baselessly claimed in part, “I don’t think what Virgil did gave DPRK any kind of real help in doing anything bad.”²³ The Ethereum Foundation

²³ *See* <https://coin.fyi/news/ethereum/ethereum-s-vitalik-buterin-to-sign-free-virgil-griffith-petition-following--e4pkte>.

initially indulged Griffith's efforts to establish a cryptocurrency mining node in North Korea. Griffith pursued this offense in part because, in the world of cryptocurrency, there are sometimes perverse rewards for breaking boundaries, disrupting the status quo, and proving that the blockchain created a zone that could escape traditional regulations. As Griffith proudly told the North Koreans, "the most valuable things we have to offer the DPRK are number one—we can give you, so blockchain gives you payments that the USA can't stop. And number two—we can give you contracts that don't go through the UN." A significant incarceratory sentence is necessary to specifically deter Griffith from using his expertise to return to these dark missions exploiting cryptocurrency technology, and it is also necessary to show Griffith's many admirers that this conduct should not be rewarded or encouraged, and that it will not be excused by the justice system.

Griffith asserts, without support, that general deterrence is not needed because "sanctions violations are not common." Def. Mem. at 41. This is wrong. As the United Nations has reported, North Korea is extensively engaged in circumventing the sanctions imposed upon it by the global community, which weakens the force of the pressure for diplomacy that those sanctions impose. *See* Panel of Expert Report at 44. North Korea does this through the aid of criminal enablers around the world. This conduct severely undermines the mission of using sanctions, economic pressure, rather than military might to achieve peace. But there will always be an economic incentive to engage in such sanctions evasion, to get access to otherwise untapped and under-developed markets, to go where no one else would, and countries under sanctions will always have an incentive to encourage, and pay a premium to, those willing to circumvent those crippling restrictions. Griffith's broad recruitment of others in the wake of his travel to the DPRK only underscores these incentives. It is only by enforcing the law, with serious consequences, that these

incentives can be adequately deterred. A Guidelines sentence is necessary to show the public that sanctions evasion will not be tolerated, and will be met with strong punishment.

General deterrence needs emphasis, particularly at this moment at time. We are witnessing a vicious war that is killing civilians for a dictator's aims. The global community has responded not with bombs, but with sanctions. Sanctions require unity. Sanctions can only work if they are fully enforced. Maximum deterrence for criminal conduct to willfully evade such critical national security measures is necessary to meet this moment.

C. The Court Should Impose a Substantial Guidelines Fine

The Court should also impose a substantial fine towards the top of the Guidelines range of \$25,000 and \$1 million. *See* PSR ¶ 110. The Guidelines provide that “[t]he court shall impose a fine in all cases, except where the defendant establishes that he is unable to pay and is not likely to become able to pay any fine.” U.S.S.G. § 5E1.2(a). When considering a fine, “[t]he burden of establishing inability to pay rests on defendant.” *United States v. Salameh*, 261 F.3d 271, 276 (2d Cir. 2001) (citing *United States v. Thompson*, 227 F.3d 43, 45 (2d Cir. 2000)).

The offense conduct and the PSR make clear that the defendant is able to pay a substantial fine. *See* PSR ¶ 100 (“Given the financial information provided, it appears the defendant is able to pay a fine.”); *id.* at p. 33 (recommending a fine of \$25,000). Griffith reported possessing more than \$1 million in assets. PSR ¶ 95. That figure, even taken as true, demonstrates that Griffith has the ability to pay a fine towards the top of the Guidelines range.

Throughout this case, however, the defendant has failed to fully report his assets, and there is cause to believe that he is continuing to fail to do so now. Griffith was remanded pending trial after he violated a court order by seeking to access one of his cryptocurrency accounts held on a U.S. exchange. Indeed, as of September 3, 2021, the defense informed the Court that this single U.S.-based cryptocurrency account possessed by the defendant was worth approximately \$1.35

million (the “U.S. Crypto Account”). Dkt. No. 143. The Government obtained records relating to that account, and determined that it is likely that account consists of only a fraction of the defendant’s assets. For example, the U.S. Crypto Account did not appear to even hold funds derived from the defendant’s salary from Ethereum. The value of the account appeared to be largely based on a single, unexplained payment received by the defendant during the time period of the conspiracy, in August 2019. Apart from that account, the defendant represented during bail proceedings in January 2020 that he held “a Singapore account, and he has cold wallets, which are basically like drives you would take and not attach[] to the Internet that I believe are located in his residence, but I believe that is under a hundred-thousand dollars.” Dkt. No. 12, 30-31. As a condition of bail, the defense agreed to “secur[e] the cryptocurrency hard drives located at the Defendant’s apartment in Singapore.” *Id.* at 54. No accounting was ever provided.

The defense has previously acknowledged that “[a]s the Court knows, a significant portion of Mr. Griffith’s savings is contained in cryptocurrency assets.” Dkt. No. 164 at 1. But Griffith’s financial holdings were only vaguely reported to Probation, and did not include any reports of current cryptocurrency holdings. PSR ¶¶ 95-100 (listing two bank accounts in addition to a foreign safety deposit box). Griffith acknowledged possessing precisely \$1 million in a safety deposit box in Singapore, which coincidentally matches the maximum fine in this case. To the extent this foreign safety-deposit box money actually consists of cryptocurrency, it should have been reported as such so that its value – which is subject to great fluctuation – could be properly considered. Similarly, Griffith reported to Probation that he “anticipates receiving an unknown amount of tokens as compensation” from the Ethereum Foundation, where he has not worked for over a year, rendering an evaluation of his true assets impossible. PSR ¶ 96. Regardless, Griffith’s self-reported \$1 million appears to be wholly separate from the additional \$1.35 million in his U.S. Crypto

Account, which was transferred to his attorney's trust account to pay unspecified legal fees in connection with this case. *See* Dkt. Nos. 164, 172. Those funds are therefore available to pay a fine. The defendant's privileged financial position, combined with the balance of the Section 3553(a) considerations described herein, warrant the imposition of a substantial fine within the Guidelines range that will serve as not only appropriate additional punishment, but also as a critical component of the general deterrence message resulting from the upcoming sentencing.

D. Griffith's Sentencing Arguments Do Not Warrant a Reduced Sentence

Griffith raises a host of arguments to seek a significantly reduced sentence. Griffith argues that his voluntary meetings with the State Department and FBI warrant credit for cooperation with the investigation, Def. Mem. at 12, that his lack of financial gain from the offense mitigates his culpability, *id.* at 32, that his "less serious" conduct renders a significant incarceratory sentence inconsistent with sentences imposed on similarly situated defendants, *id.* at 28-29, and that a sentence within the Guidelines sentencing range would be inherently disparate in light of statistics showing that a substantial percentage of sentences imposed in this District are below the applicable Guidelines ranges, *id.* at 29. None of these arguments warrant the extraordinary leniency Griffith seeks.

1. Griffith's Contacts with Law Enforcement Do Not Mitigate His Conduct

The defense assertion that Griffith "cooperated extensively" with law enforcement to "rectify his prior actions" rings hollow in the face of Griffith's own contemporaneous statements and deceptive acts to continue the conspiracy at the same time he was allegedly "assist[ing] the U.S. government." Def. Mem. at 12, 14. Griffith contacted U.S. government authorities out of self-interest after the Conference, and attempted to mislead them about his own criminal activities. For example, in June 2019, Griffith wrote in an email to CC-1 that he had gone to the U.S. Embassy

because he was “too high profile for the US Gov not to know” that he had defied their warnings and traveled to North Korea. GX 3065. Similarly, in May 2019, Griffith informed a friend via Facebook that he was planning to meet with the FBI regarding North Korea because “I’ve already technically violated the law [a]nd violated sanctions.” GX 2417. Similarly, before meeting with FBI, Griffith messaged CC-2 about his plan for limiting his disclosures to U.S. law enforcement, saying “it’s too implausible that getting around sanctions didn’t come up. I was planning to say something like, ‘The capacity for getting around sanctions came up in discussing. But it was almost entirely about doing a demo of ‘economic reunification’ with South Korea.’ This seems vastly less objectionable while also being *mostly* true.” USAO_00944 (emphasis added).

Griffith then concealed the true extent of his own conduct at his meetings with the FBI. Griffith purported to report on North Korea’s interest in sanctions evasion, but carefully omitted his own role in advising the North Korean audience at the Conference on precisely how to use cryptocurrency to evade sanctions. For example, Griffith informed the FBI that he believed North Korea was interested in using cryptocurrency for sanctions evasion, but omitted the fact that Griffith *himself* was the person to map out how to do so for the North Korean audience, alongside CC-2. Griffith initially described giving one presentation on “Blockchain and Peace,” when in reality he gave additional presentations on the second day of the Conference.

Griffith did not seek to truly cooperate but rather to conduct damage control. Days after his November meeting with the FBI, Griffith told a contact “I want to get a second passport asap. I didn’t like having my back against the wall.” He proposed to buy “a passport from St. Kitts for 100k USD.” He contemplated renouncing his U.S. citizenship. Griffith was seeking ways to avoid accountability to U.S. authorities.

Griffith brazenly perpetuated the aims of the conspiracy even in the face of law enforcement's clear warnings. On February 27, 2019, the State Department specifically denied Griffith permission to participate in the Conference, informing him that "your request is not in the national interest of the United States." (*See* GX 3041 & 3041A). Griffith went anyway, knowing that the purpose of the Conference was sanctions evasion. *See, e.g.*, GX 2408. In May 2019, the FBI admonished Griffith to cease violating the sanctions on North Korea. Griffith ignored that warning, and persisted in his efforts to recruit experts to travel to North Korea, to aid and abet plans for a second cryptocurrency conference to be held in Pyongyang in 2020, and to pursue other ways to work with North Korea, including by illegally funding travel for North Koreans to technology industry events. Griffith's participation in the criminal conspiracy was only disrupted by his arrest in November 2019. Since that time, Griffith has never made any effort to cooperate with law enforcement and resisted accepting responsibility for this crime until the morning of trial.

Griffith's consent to permit law enforcement to search his cellphone and GoPro footage merits little consideration, because Griffith knew that these devices contained only limited information since he had used "burner" electronic devices while in North Korea and communicated via encrypted platforms such as Telegram. Griffith deleted his Telegram account, and his messages were only recovered through another witness. Griffith's burner laptop was eventually recovered by Singaporean authorities, from a third party, and evidence obtained from that laptop was provided to the FBI, without any voluntary assistance by Griffith. Griffith's burner cellphone was never recovered by U.S. authorities. Griffith's communications with Individual-1²⁴ regarding providing the DPRK with hardware wallets and creating smart contracts designed for them, for

²⁴ Individual-1 has submitted a letter in support of Griffith in connection with sentencing, without reference to this conduct.

example, were made using that burner phone and obtained only through alternative means. Indeed, when another one of Griffith's cellphones was seized in Singapore, Griffith took steps to explicitly block Singaporean law enforcement from sharing the evidence contained in that phone with U.S. law enforcement. When Griffith was arrested in Los Angeles, he asked the arresting agent to power off his cellphone, in an apparent attempt to thwart the FBI's ability to search it later.

Even while incarcerated, Griffith has remained defiant. On one prison call, Griffith contacted a friend, who promptly notified Griffith that the call was on speakerphone and his young children were with him. Griffith then told the children, "Don't do drugs. Don't go to jail. Don't talk to the FBI." His friend then commented, "Don't go to North Korea." USAO_010443 (79038112_Sep_16_2021_15_16_07_PM_5415171592.wav). Even this interaction shows that Griffith's primary regret is getting caught. His message to a friend, and even to children, was to *avoid* cooperation with law enforcement.

Griffith's limited voluntary disclosures to the FBI and the State Department generally reflect an effort by Griffith to control the narrative, dodge responsibility for his crimes, and deflect attention from his own ongoing misconduct. They do not credibly indicate any genuine effort to cooperate with law enforcement or to impede the threat posed by North Korea to the United States. Griffith's August 7, 2019 audio messages, in which he referred to his assistance to the DPRK as a "game" and bragged that "it seems like the Americans let you get away with it once" as he continued to pursue the objects of the conspiracy, encapsulates his self-interested strategy and disrespect for law enforcement. GX 1107A, 1107B. Those words speak volumes. They reflect no contrition, no remorse, and no intent to aid law enforcement. To the contrary, Griffith's misleading engagement with law enforcement militates in favor of a significant sentence to reflect Griffith's

efforts to avoid responsibility for his actions and to serve as a clear warning to any other potential offender standing in Griffith's shoes.²⁵

2. Griffith's Commission of the Crime For Free Fails to Mitigate His Conduct

Griffith's emphasis that he was not paid to commit his crime is an unpersuasive distraction. Def. Mem. 32. First, Griffith actually offered to use his independent wealth and industry position to *pay others* in order to induce them to advance the goals of the conspiracy. Griffith offered to pay up to \$10,000 to set up a cryptocurrency mining node in North Korea, to "crowd-fund" travel for North Korean representatives, and to broker deals with software developers working with Griffith in which a cut of the proceeds could be negotiated later if North Korea could not pay for it. *See supra* 8, 30-31, 37. Funding crime is no less disturbing than profiting from crime. Second, Griffith's willingness to participate in this crime, at his own expense, only demonstrates the troubling degree to which he was eager to engage in dangerous criminal activity. Griffith possessed substantial wealth, a stable income in a legitimate job, and the extraordinary privileges attendant to his doctorate-level education. Griffith's choice to invest those advantages in this crime constitutes an aggravating factor in this case.

Third, the evidence indicates that Griffith did believe that the conspiracy could reap financial benefits for him and its other participants in the future, even if he was not paid now. When pursuing the node, for example, Griffith emphasized that "[t]his could turn into a mildly

²⁵ Griffith also cites his prior engagement with the U.S. government prior to the offense on unrelated matters as evidence of his "assistance to law enforcement." Def. Mem. 15. The Government has not been able to verify these claims, but agrees that these matters can be considered by the Court as part of Griffith's personal history and characteristics, just as the Court may consider Griffith's admitted failure to file U.S. taxes for years and interest in purchasing citizenship abroad to avoid U.S. liabilities. Nonetheless, the Government submits that Griffith's behavior with respect to the charged conduct is most relevant for sentencing.

lucrative little business for whoever does this.” GX 3003. Griffith used the Conference to advertise a particular product, the “NeverSlash,” which at the time, he was helping to develop, market, and sell. GX 3086; 3057. As Griffith told CC-3, his plans made “economic sense” because they would “help” North Korea “circumvent the current sanctions on them.” PSR ¶ 18. Griffith also wrote in his notes at the conference that he intended to purchase certain North Korean websites, including blockchain.kp and cypto.kp, which would later be used by North Koreans utilizing blockchain and cryptocurrency. GX 810. And he also utilized the conference to bolster his personal brand as a risktaker and as a means to highlight the unregulatable nature of the cryptocurrency created by his employer, the Ethereum Foundation. For example, Griffith discussed his trip to North Korea openly, wearing the suit that he has commissioned for him in the DPRK to industry events including the May 2019 Ethereum Summit in Brooklyn. Whether or not Griffith was actually paid for his participation in the conspiracy, the evidence demonstrates that Griffith acted out of his own perceived self-interest, including the possibility of gaining future financial rewards.

3. Griffith’s Offense Exceeded “Providing Publicly Known Oral Information”

Griffith’s self-serving attempt to characterize his offense as “providing publicly known oral information” and to disclaim the utility of his services to the DPRK is contradicted by the record of his own statements at the time of the offense. Def. Mem at 32. Griffith introduced himself to the North Korean audience by expressly emphasizing “the most valuable things we have to offer the DPRK” such as “payments that the USA can’t stop” and “contracts that don’t go through the UN.” Griffith declared that “we definitely think this will be *really useful for the DPRK, and that’s why we’re here.*” Contrary to Griffith’s claims now that his presentation covered only well-worn topics and techniques, Griffith told his audience then that “if the DPRK adopts this [blockchain

technology], they will be on the very leading edge of technology.” And of course, Griffith pleaded guilty to this offense, admitting that he provided services that exceeded mere “information.”

Griffith’s arguments, moreover, rely on abject speculation unsupported by the evidence to distract from his willfully criminal intentions and the seriousness of his crime. Griffith offers sheer conjecture to argue that his tailored presentations at the Conference were of little use to the participants, and to the North Korean regime. Once again, Griffith’s own contemporaneous statements completely belie his attempts to advance that false narrative now. At the time, Griffith wrote of the North Koreans, “they seemingly know nothing” and that the “tech is pretty weak.” GX 2303. In another conversation, when a friend asked Griffith “how active is NK crypto in reality[?],” Griffith responded, “its negligible” but that “they are interested in using crypto to get around sanctions.” GX 2413. Griffith circulated a paper to his co-conspirators that expressly opined that cryptocurrency use by North Korea was only just becoming a threat that, at the time of the Conference, “likely only play[ed] a peripheral role” but presented grave increased risks for the future. GX 2613. All of this evidence strongly indicates that Griffith acted with the understanding that he was presenting emerging technology and sanctions-evasions techniques to his audience, and that was by design to serve the conspiracy. Griffith intended to perform a useful service for the North Koreans, and he delivered that service.

Moreover, the evidence demonstrates, and Griffith acknowledged to the FBI, that the audience was comprised at least in part of North Korean government officials, and that the Conference was designed in coordination with the North Korean government. The logical implication is that Griffith knew that the North Korean government endorsed and prepared the Conference to serve ends useful to the regime. As CC-1 emphasized to Griffith, on or about June 10, 2019, “Please understand that your permission to enter the DPRK was absolutely exceptional

and through my very personal guarantee (Because I trust [CC-2] and he trusts you). . . . the absolute majority of our officials cannot engage with any U.S. person in regular circumstances.” GX 3066. Without a strong utility for the regime, it would make little sense for North Korea, a highly controlled dictatorship and hermetic state, to open its doors to Griffith and his cohort of foreigners, to permit them the rare opportunity to interact with North Korean government officials, and to devote its government resources to the Conference.

It is impossible to measure the actual damage to national security caused by Griffith’s crime. But the evidence shows that Griffith’s explicit mission consisted of teaching his North Korean audience specific techniques to evade the U.S. sanctions. Griffith’s intended actions undoubtedly served to undermine the U.S. government’s systemic ability to enforce sanctions against North Korea by mapping out the means for his North Korean audience to move money outside of the traditional, highly regulated banking system and hide it through anonymous cryptocurrency transactions. Griffith was featured as an “expert” and a “scientist” with special skills who had helped make it “possible to transfer money across any country in the world regardless of what sanctions or any penalties that are put on any country by any other country,” so that “the DPRK can freely move money around the world without the U.S. blocking any of these transactions.” GX 403-A. Griffith delivered on this promise by presenting on precisely how the North Korean audience could evade U.S. sanctions through the use of cryptocurrency, offering instructions, examples, and participating in question-and-answer sessions. Griffith and his co-conspirators also promoted North Korea’s creation of its own cryptocurrency coin for this same sanctions-evading purpose, and offered up their collective assistance to accomplish that goal. Griffith’s contemporaneous statements show that he knew his participation in the conspiracy risked advancing North Korea’s use of cryptocurrency or blockchain technology to serve its

nefarious purposes, including its nuclear program and drug trade. Griffith nonetheless acted with total disregard for the potentially disastrous consequences of these actions.

Griffith's services with respect to smart-contracts risked severe harms as well. Griffith specifically pitched the DPRK audience on the "idea" that they could gain leverage in sanctions negotiations against the United States by placing a "module on a missile" to "deactivate" the missile, but only "if you [i.e., the United States] get rid of the sanction, the missile are really gone." Griffith also pitched the use of the same technology to leverage the DPRK's control over missiles to negotiate for "less artillery in the DMZ," that is, weapons in the Korean Peninsula's Demilitarized Zone, for the DPRK's benefit. Griffith sought to aid the DPRK to "to make foreign journalists put a deposit on Augur that is forfeited if they write a highly unflattering article," a measure that would strengthen the DPRK's propaganda machine, and offered to introduce his handler, a DPRK government official, to software developers for this purpose.

Under the claimed guise of providing this Court with background information about cryptocurrency terms and technology, the defendant submits an affidavit from a Cyprus-based purported expert, Andreas M. Antonopoulous, stating in part that "nothing about the information presented by Mr. Griffith or others during the Conference was tailored to or otherwise unique to that particular event or locale." Def. Mem. Ex. E ¶ 20. This claim is refuted by the evidence, and stands at irreconcilable odds with the defendant's own guilty plea. In his allocution, the defendant stated in part that he had violated the law because "[s]pecifically, I delivered a presentation on blockchain technology was that was tailored to a North Korea audience in April 2019," and confirmed that he knew what he was doing was wrong and unlawful. Griffith's submission of the Antonopoulous Declaration and his arguments diminishing the severity of his conduct are unavailing, and serve only to undermine Griffith's acceptance of responsibility.

4. Comparable Sentences

Lastly, a Guidelines sentence in this case would not create “significant disparities in treatment between similarly situated inmates” as the defense asserts. Def. Mem. 28-29. In support of its position, the defense claims that many defendants have received “downward variances for similar offenses” and relies on comparisons to *United States v. Banki*, Case No. 10 cr-00008 (S.D.N.Y. 2010), *United States v. Amirnazmi*, Case No. 08-cr-00429, (E.D. Pa. 2010) and *Sarvestani v. United States*, 2015 WL 7587359 (S.D.N.Y. Nov. 25, 2015). Def. Mem. at 29.

First, the Government notes that other defendants in this District have similarly relied on the same downward variances granted to Banki, Amirnazmi, and Sarvestani, and charts much like the one included by Griffith here. *See, e.g., United States v. Atilla*, 15 Cr. 867 (RMB) (Dkt. No. 498, Defense Sentencing Br. at 45-51).²⁶ Such surveys are of limited utility. Sentencing is an individualized proceeding that depends on the applicable Guidelines range, the nature and circumstances of the offense, the history and characteristics of the defendant, and numerous other factors that are particular to each case. They can be significantly impacted by, for example, whether the defendant cooperated and received a Section 5K1.1 letter. These lengthy charts, which are devoid of significant details, are unhelpful in making comparisons and appears to be an attempt to swallow careful consideration of the facts in this case. Moreover, to the extent there is any discernable trend of downward variances in IEEPA cases, such a trend may very well have contributed to the failure of deterrence seen in Griffith’s own words and deeds in this case. The reasons for granting a downward variance in the past, for wholly different conduct and wholly different defendants, may not meet the ends of sentencing facing the Court today.

²⁶ Like Griffith, Atilla also attached a chart, the selection methodology of which is unexplained and which he acknowledged was not comprehensive, of other sentences imposed in various sanctions prosecutions. *Id.* at 50-51 & Ex. B.

Regardless, *Banki*, *Amirnazmi*, and *Sarvestani* each featured factors that readily distinguish them from Griffith. As an initial matter, Banki's conviction was vacated and the sentence imposed is therefore of extremely limited value for this Court's consideration. *United States v. Banki*, 685 F.3d 99, 108-15 (2d Cir. 2012) (vacating convictions for conspiring to violate the IEEPA and operating as an unlicensed money remitter). But even on its facts, *Banki* is otherwise easily distinguishable. Between approximately May 2006 and September 2009, Banki participated in hawala transfers in which an individual or entity would transfer funds to Banki's bank account in the United States, and a family member in Iran would disburse a corresponding amount to a recipient in Iran. *Id.* at 103-04. Banki contended that these transfers, totaling approximately \$3.4 million in the aggregate, were simply family remittances permitted by a general license for such transfers and, indeed, the trial court's failure to instruct the jury on the family-remittance license was the basis for the Second Circuit's vacatur of his IEEPA conviction. *Id.* at 109-12. Banki received a presidential pardon in January 2021.

Amirnazmi pursued an ambitious goal to transform Iran "into an independent chemical powerhouse," *United States v. Amirnazmi*, 645 F.3d 564, 567 (3d Cir. 2011), though his actual achievements fell short of this aim. The sentencing court noted that, "I do not think he is very effective." *United States v. Amirnazmi*, 08 Cr. 429 (CMR) (E.D. Pa. Feb. 17, 2010) (Dkt. No. 195 at 108). At sentencing, the court gave significant weight to Amirnazmi's advanced age and significant medical conditions, factors that are not present here. *Amirnazmi*, 08 Cr. 429 (CMR) (E.D.Pa. Feb. 17, 2010) (Dkt. No. 195 at 106-07, 114); *see also id.* at 83-84.

Sarvestani supplied satellite equipment to Iranian companies, and some of those sales included parts that were sourced from the United States. *United States v. Sarvestani*, 13 Cr. 214 (PGG) (S.D.N.Y. Sept. 12, 2013) (Dkt. No. 45 at 4-5). Sarvestani contended that the satellite

equipment was sold to a provider of residential internet and communications services, *id.* at 8-9, 19, though the Government argued that there were at least some potentially non-residential applications of the equipment. *Id.* at 16; *see also id.* at 24. Notably, after his arrest, Sarvestani met with law enforcement in an effort to provide substantial assistance, though these efforts did not result in a cooperation agreement or motion pursuant to § 5K1.1 of the Guidelines. *Id.* at 7. While Griffith argues he should receive credit for his voluntary meetings with the FBI, Griffith made no effort to cooperate with the Government following his arrest in stark contrast to Sarvestani. In addition to a below-Guidelines, but still comparatively substantial, sentence of 30 months' imprisonment, the court also imposed a fine at the top of the Guidelines range. *Id.* at 28.

In short, none of these defendants' circumstances provide a particularly apt comparison to Griffith. Indeed, each of the defendants has at least one highly notable mitigating circumstance lacking in this case: Banki's convictions were vacated, Amirnazmi suffered from advanced age and serious medical and psychological conditions, and Sarvestani attempted (albeit unsuccessfully) to cooperate with the prosecution upon his arrest. Griffith, of course, does not discuss the substantial sentences imposed on other IEEPA violators who participated in actual acts of money laundering and sanctions evasion, such as he encouraged through his services. Such cases include Rafil Dhafir, who was sentenced to 264 months for conspiring to launder several million dollars to Iraq, 03 Cr. 64 (NAM) (N.D.N.Y.); and Vikram Datta, who was sentenced to 235 months for conspiring to launder millions in drug proceeds, 11 Cr. 102 (LAK) (S.D.N.Y.), demonstrating that downward variances are not – and more importantly, should not be – routinely granted in IEEPA cases.

But as sentences imposed in different cases, with different facts and circumstances, make clear, an understanding of the diversity of defendants and their conduct does not require sacrificing

