UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA	:	
- v. -	:	
VIRGIL GRIFFITH,	:	20 Cr. 15 (PKC)
Defendant.	:	

GOVERNMENT'S MOTIONS *IN LIMINE*

AUDREY STRAUSS
United States Attorney for the
Southern District of New York
One St. Andrew's Plaza
New York, New York 10007

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

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

Rules

The Government respectfully submits this memorandum in support of motions *in limine* seeking the following rulings with respect to the upcoming trial of defendant Virgil Griffith:

1. Evidence of Griffith's 2018 attempts to place cryptocurrency infrastructure in the Democratic People's Republic of Korea ("DPRK"), illegal use of his U.S. passport, attempt to facilitate a cryptocurrency transaction with the DPRK, statements about his taxes, and statements regarding the renunciation of Griffith's U.S. citizenship are admissible as direct evidence of the charged conspiracy and, alternatively, are admissible pursuant to Federal Rule of Evidence 404(b).

2. Statements of Griffith's co-conspirators, who participated with Griffith in the charged scheme to provide services to the DPRK, and evade and avoid U.S. sanctions on the DPRK, should be admitted as co-conspirator statements pursuant to Federal Rule of Evidence 801(d)(2)(E) and as statements against interest pursuant to Federal Rule of Evidence 804(b)(3).

3. Statements made by other individuals during communications with Griffith are admissible for the limited purpose of providing context for and understanding of Griffith's statements, and are not offered for the truth of the matters asserted.

4. Extraneous evidence regarding the cryptocurrency capabilities of the DPRK should be precluded.

For the reasons set forth below, the Court should grant the Government's motions.

BACKGROUND

On November 21, 2019, Griffith was charged in a criminal Complaint with conspiring to violate the International Emergency Economic Powers Act ("IEEPA"), 50 U.S.C. §§ 1701-1706. One week later, Griffith was arrested in Los Angeles pursuant to the charge in the Complaint. On January 7, 2020, a Grand Jury sitting in this District returned an Indictment charging the defendant with one count of conspiring, from at least approximately August 2018 to November 2019, to violate IEEPA and the North Korea Sanctions Regulations ("NKSR") by providing services to the DPRK or DPRK persons without obtaining a license to do so, and by evading and avoiding the requirements of U.S. law with respect to the provision of services to the DPRK. The Government anticipates that the evidence at trial will show that the defendant, starting as early as February

2018, plotted with others to illegally provide services to the DPRK and DPRK persons, without a license and in contravention of the 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.

At trial, the Government will establish these facts through, among other evidence, 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, and video from inside the DPRK, and law enforcement and civilian witness testimony.

I. The Charged Conspiracy to Violate IEEPA

A. 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. At the time, Griffith, an American citizen, was living in Singapore and employed as a "Senior Researcher" at the Ethereum Foundation, an international cryptocurrency organization and creator of a cryptocurrency bearing the same name (ether). Griffith's responsibilities at the Ethereum Foundation included business development. As early as February 17, 2018,[1] and as reflected in emails and other communications that the Government intends to introduce at trial, Griffith proposed a plan to provide cryptocurrency services in the DPRK to a Singaporean contact ("Co-Conspirator-3" or "CC-3")[2] 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."[3] 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."[4] CC-3 agreed to assist.

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,

---

[1] Because participants in the messages described herein were often in different time zones, the dates referenced throughout this brief are those reflected in Griffith's communications.

[2] The Government has produced the communications referenced in this brief in discovery and provided to the defense the identity of each of the co-conspirators referenced herein.

As described in the Complaint and below, *see infra* 8, CC-1 and CC-2, the co-organizers of the Conference, are defined in the Complaint. As described in greater detail below, CC-1 is a representative of the DPRK and CC-2 is a cryptocurrency professional.

[3] 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 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.

[4] Communications quoted herein appear as in the original unless otherwise indicated.

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 . . . ." 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." Until they figured out the intermediary, however, Griffith wrote that the project "will be supported by myself, an individual." Anticipating a potential issue, Griffith acknowledged that he was "a US citizen, but I'll be funnelin[g] things through Singapore/China to avoid any problems from that." 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."

CC-4 responded that day with some skepticism, noting that setting up a node in the DPRK would be "incredibly difficult." CC-4 told Griffith that such 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.

Griffith was undeterred. 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." 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!" 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."

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. 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." 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." 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." 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."

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." 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." 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?" It appears that CC-4 did not respond in writing. 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." In response, CC-3 wrote, "One step closer."

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?" 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"). Individual-1 and Individual-2 appear to have discouraged Griffith from proceeding with the node. 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." But Griffith did no such thing.

Instead, 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. 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[.]"

Griffith also began researching travel to the DPRK. 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?" An email address with the username "Special Delegation-DPR of Korea" sent a response stating, "Yes, no problem." Griffith responded: "Wait really? I presumed that was impossible. Have American citizens previously visited under similar programs?" The sender answered, "No. It is the first time." The next day, Griffith contacted by email CC-2, who advised Griffith that "the dprk will not stamp your passport" if Griffith elected to travel to the Conference.

Griffith next made plans to travel to North Korea, and discussed his plans to participate in the Conference. On August 31, 2018, one of Griffith's friends ("Individual-3") asked in an email exchange why he was willing to risk his safety to go to a conference in the DPRK. 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." In response, Individual-3 asked, "What if they're funding their drug trade and nuclear program with crypto?" Griffith replied, "Unlikely. But they'd probably like to start doing such." 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."

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 a dark-web software entity (the "Dark Web Entity"), 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, [Dark Web Entity] doesn't mind being edgy in these ways. If [Dark Web Entity servers] or others would like to crowdfund putting a [Dark Web Entity] node in DPRK, I bet they'd do it under the same conditions described below.

> 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.

B. 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." 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.

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

On December 19, 2018, Griffith submitted his initial payment for the Conference and forwarded proof of the same to the DPRK Email Account. At all times relevant to the charged conduct, 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.[5] 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. 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.'"

On January 25, 2019, Griffith wrote to the U.S. State Department's Special Validations office, on the letterhead of a Singapore-based company, seeking permission to travel to the DPRK, stating, "I have been accepted to speak at the Pyongyang Blockchain and Cryptocurrency Conference, and I wish to do so." Griffith further 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." The U.S. State Department denied Griffith's application.

On January 27, 2019, Griffith wrote to CC-3 that he was going "[t]o meet with SGians

[5] *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").

[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: Mr. Kim Won Il, Committee for Cultural Relations with Foreign Countries·. You also have to send them your passport, personal details and CV (Resume).

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: Mr. Kim Won Il, Committee for Cultural Relations with Foreign Countries. I attach my passport, and CV.

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." 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." 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." On March 8, 2019, underscoring the importance of sending the email to New York, CC-1 wrote, "Just making

sure that [CC-2] told you the correct (updated) e-mail address of our DPRK mission in NY. If you send to the old one, please make a resend to this new one." In response, Griffith wrote, "Already on it."

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's UN Mission in Manhattan.

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. 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.

C. Griffith's Attendance and Presentation at the Conference

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

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 contracts and the DPRK's own cryptocurrency coin;

and acting as brokers to connect Conference attendees and participants with cryptocurrency equipment, service providers, and experts. 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"). Griffith later referred to CC-6 as a "minder" in his FBI interviews.

At trial, the Government will introduce various forms of contemporaneous evidence of what transpired at the Conference. The Government's evidence will include audio recordings from the Conference, video clips of the Conference and the defendant's remarks, notes written by Griffith for his presentation, images of Griffith's writings on a whiteboard for the participants, and communications sent by Griffith to others during his time in the DPRK.

At 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.
>
> 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.[6]

[6] Transcripts of the recordings containing the content of presentations made at the Conference are in draft form and are subject to change as they are finalized in advance of trial.

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 county 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[7] idea. . . .

[7] *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

> 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." Based on photographs taken at the Conference, Griffith also appears to have described a cryptocurrency security project that he had been working on, encouraging Conference attendees to view the product's website.

After Griffith's presentation, 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 way in which those technologies could be used to evade sanctions. 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

---

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 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.

The 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.

D. 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.

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 minder. Griffith then wrote to CC-5 on Facebook asking her to "send us the Korean language materials." 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 1ETH[8]

[8] ETH is the symbol for ether, the unit of cryptocurrency created by the Ethereum Foundation.

forward and back." Griffith also attempted to recruit other cryptocurrency professionals to travel to the DPRK in order to provide similar services to the DPRK. Within just one day of leaving the DPRK, 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." 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. 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. If you 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.

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." On May 16, 2019, CC-1 wrote to Griffith, stating that "the situation is still serious (Max Thunder military exercises)[9] 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."

[9] 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.

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

E. Griffith's Statements to Law Enforcement after the Conference

After the Conference, 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 UN Mission in Manhattan to facilitate his travel, and that he sent the requested documents for travel to the DPRK UN 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's 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, audio recordings from the Conference capture CC-2 and Griffith speaking together to Conference attendees regarding OTC exchanges of cryptocurrency.

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. The agents advised Griffith that doing so would likely violate U.S. law, to include the prohibitions associated with IEEPA.

F. 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. For instance, on August 4, 2019, Griffith wrote CC-2, "I'd like to do the sending of the l ETH between Pyonyang and Seoul. And it seems the only way to get that to happen is for us to take another trip to DPRK." 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 wrote, "Ethereum Foundation can't touch anything DPRK. B[u]t 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.

The next day, on August 7, 2019, Griffith sent an audio recording to Individual-5, in which Griffith stated: "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."

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].” 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.” 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. 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.” On October 28, 2019, Griffith wrote to Individual-5, “I’m trying to bring DPRK, representing .KP, to Australia,” referring to the travel for a “delegation” that Griffith had proposed to fund.

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.” 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.” 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.”

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."

II. Background on IEEPA and the Elements of the Charged Offense

IEEPA 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). Criminal penalties under IEEPA apply to those who "willfully commit[], willfully attempt[ ] to commit, or willfully conspire[ ] to commit" a violation of any license, order or regulation issued pursuant to IEEPA. *Id.* § 1705(c). IEEPA exempts those who act in "good faith" reliance on IEEPA, or on "any regulation, instruction, or direction" issued under IEEPA, from both civil and criminal liability. *Id.* § 1702(a)(3).

Beginning with Executive Order 13466, issued on June 26, 2008, the President found that the situation "on the Korean Peninsula constitute[s] an unusual and extraordinary threat to the national security and foreign policy of the United States and . . . declare[d] a national emergency to deal with that threat." Exec. Order 13466. Following the issuance of Executive Order 13466, the U.S. Department of Treasury, Office of Foreign Assets Control ("OFAC") promulgated the NKSR to implement sanctions on the DPRK. *See* 31 C.F.R. Part 510.

On August 30, 2010, the President "expand[ed] the scope of the national emergency declared in Executive Order 13466" finding that

> the continued actions and policies of the Government of North Korea, manifested most recently by 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 announced test of a nuclear device and its missile launches in 2009; its . . . procurement of luxury goods; and 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, destabilize the Korean peninsula and imperil U.S. Armed Forces, allies, and trading partners in the region, and thereby constitute an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States.

Exec. Order 13551. In light of these harms, the President authorized the sanctioning of additional individuals who, for example, "directly or indirectly, engaged in money laundering, the counterfeiting of goods or currency, bulk cash smuggling, narcotics trafficking, or other illicit economic activity that involves or supports the Government of North Korea or any senior official thereof." *Id*. The President again authorized additional sanctions on January 2, 2015, citing the DPRK's "destructive, coercive cyber-related actions . . . and commission of serious human rights abuses [that] constitute a continuing threat to the national security, foreign policy, and economy of the United States." Exec. Order 13687.

On March 18, 2016, the President issued Executive Order 13722, which imposed comprehensive sanctions on North Korea. It stated that "the Government of North Korea's continuing pursuit of its nuclear and missile programs, as evidenced most recently by its February 7, 2016, launch using ballistic missile technology and its January 6, 2016, nuclear test . . . increasingly imperils the United States and its allies." Exec. Order 13722. Accordingly, the Executive Order imposed an embargo, which prohibited "the exportation or reexportation, direct or indirect, from the United States, or by a United States person, wherever located, of any goods, services, or technology to North Korea" and "any approval, financing, facilitation, or guarantee by a United States person, wherever located, of a transaction by a foreign person where the transaction by that foreign person would be prohibited by this section if performed by a United States person or within the United States." *Id*.

Pursuant to Executive Order 13722, and to incorporate certain other legislation, OFAC amended and reissued the NKSR on March 5, 2018. 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).

OFAC's regulations further state that the "prohibition on the exportation and reexportation of goods, services, or technology . . . applies to services performed on behalf of a person in North Korea or the Government of North Korea or where the benefit of such service is otherwise received in North Korea, if such services are performed . . . by a U.S. person." 31 C.F.R. § 510.405(a). The regulations also state that "U.S. persons may not, except as authorized by or pursuant to this part, provide legal, accounting, financial, brokering, freight forwarding, transportation, public relations, or *other services* to any person in North Korea or to the Government of North Korea." *Id*. § 510.405(d)(1) (emphasis added). The defense does not dispute that Griffith is a U.S. person under these regulations.

To prove the defendant guilty of conspiring to violate IEEPA as charged in the Indictment, the Government must establish first the existence of a conspiracy with the objective either to provide services to the DPRK without obtaining a license to do so, or to evade and avoid the requirements of U.S. law with respect to the provision of services to the DPRK; and second that the defendant knowingly and willfully became a member of that conspiracy, with knowledge of at least one of its unlawful objectives.

DISCUSSION

I. Evidence of Griffith's Pre- and Post-Conference Efforts to Assist the DPRK, Illegal Use of a Passport, Statements Regarding Renunciation of Griffith's U.S. Citizenship, and Statements About Griffith's Taxes Are Admissible as Direct Evidence and Pursuant to Rule 404(b)

At trial, the Government seeks to admit as direct evidence of the charged crime, or in the alternative, pursuant to Rule 404(b), the following categories of evidence described in greater detail above:

1. Griffith's 2018 efforts to provide services to the DPRK, including by establishing a cryptocurrency mining node in the DPRK, *see supra* 2-8;

2. Griffith's illegal misuse of his U.S. passport by traveling to the DPRK without a special validation visa, and his attempt to prevent his DPRK visa from appearing on his U.S. passport, *see supra* 11;

3. Griffith's post-Conference efforts to provide services to the DPRK, including by attempting to facilitate a financial transaction of 1 ether with the DPRK, assisting in the promotion of a second cryptocurrency conference to be held in the DPRK in 2020, recruiting others to travel to the DPRK to provide cryptocurrency-related services to the DPRK on his behalf, and attempting to fund travel for DPRK persons, *see supra* 21-23; and

4. Griffith's statements regarding his interest in renouncing his U.S. citizenship, purchasing citizenship elsewhere, his failure to pay taxes, and setting up a money laundering company in North Korea, *see supra* 23-24.

All of this evidence constitutes direct proof of the charged conspiracy, which spanned an extended period beginning in 2018 and continuing until the defendant's arrest in November 2019. Each of these categories of evidence arose out of the same series of events as the charged conduct, will be necessary to complete the story of the crime on trial, and to provide background for the events alleged in the Indictment. In the alternative, the evidence identified above is also admissible pursuant to Rule 404(b) to prove the defendant's motive, opportunity, intent, preparation, plan,

knowledge, identity, and absence of mistake or accident with respect to the conspiracy charged in the Indictment.[10]

A. Legal Standard

Relevant evidence "need only tend to prove the government's case," such as "evidence that adds context and dimension to the government's proof of the charges." *United States v. Gonzalez*, 110 F.3d 936, 941 (2d Cir. 1997). Thus, background evidence is relevant and admissible, pursuant to Rule 401, where it tends "to show, for example, the circumstances surrounding the events or to furnish an explanation of the understanding or intent with which certain acts were performed." *Id.* (internal quotation marks omitted). Evidence is also admissible if it relates to conduct that: (i) "'arose out of the same transaction or series of transactions as the charged offense'"; (ii) "'is inextricably intertwined with the evidence regarding the charged offense'"; or (iii) "'is necessary to complete the story of the crime on trial.'" *United States v. Gohari*, 227 F. Supp. 3d 313, 317 (S.D.N.Y. 2017) (quoting *United States v. Robinson*, 702 F.3d 22, 36-37 (2d Cir. 2012)). "Evidence fitting within one of these three categories is considered direct evidence and Rule 404 is not applicable." *United States v. Fiumano*, No. 14 Cr. 518, 2016 WL 1629356, at *3 (S.D.N.Y. Apr. 25, 2016). In particular, it is well settled in the Second Circuit that where, as here, an indictment contains a conspiracy charge, "[a]n act that is alleged to have been done in furtherance of the alleged conspiracy" is considered "part of the very act charged." *United States v. Diaz*, 176 F.3d 52, 79 (2d Cir. 1999) (internal quotation marks omitted); *see United States v. Thai*, 29 F.3d

[10] The Government hereby also provides notice of its intent to offer this evidence pursuant to Rule 404(b). The Government plans to continue to meet with potential witnesses between now and trial, and the Government will supplement this notice as necessary should the Government learn of additional Rule 404(b) evidence that it plans to offer, and/or should the Government seek to introduce additional evidence pursuant to Rule 404(b) in response to evidence or arguments offered by the defense at trial.

785, 812 (2d Cir. 1994) (explaining that "uncharged acts may be admissible as direct evidence of the conspiracy itself").

Moreover, evidence is "not other act evidence within the meaning of Rule 404(b)" if it is "admissible to prove material facts other than [the defendant's] propensity to commit a crime." *United States v. Concepcion*, 983 F.2d 369, 392 (2d Cir. 1992). Indeed, relevant evidence is "not confined to that which directly establishes an element of the crime." *Gonzalez*, 110 F.3d at 941; *see also United States v. Inserra*, 34 F.3d 83, 89 (2d Cir. 1994) ("[E]vidence of other bad acts may be admitted to provide the jury with the complete story of the crimes charged by demonstrating the context of certain events relevant to the charged offense."). Such evidence need not "directly establish an element of the offense charged." *United States v. Segui*, No. 19 Cr. 188 (KAM), 2019 WL 8587291, at *6 (E.D.N.Y. Dec. 2, 2019) (quoting *United States v. Daly*, 842 F.2d 1380, 1388 (2d Cir. 1988)). Instead, it may be used "to provide background for the events alleged in the indictment," such as "the circumstances surrounding the events or to furnish an explanation of the understanding or intent with which certain acts were performed." *Id*.

Alternatively, under Rule 404(b), evidence of a defendant's "other crimes, wrongs, or acts" is admissible when offered for a proper purpose other than the defendant's criminal propensity. *See, e.g., United States v. Germosen*, 139 F. 3d 120, 127 (2d Cir. 1998); *United States v. Levy*, 731 F.2d 997, 1002 (2d Cir. 1984). Rule 404(b) contains a non-exhaustive list of proper purposes for which "other act or crime" evidence may be admitted, including "motive, opportunity, intent, preparation, plan, knowledge, identity or absence of mistake or accident." Fed. R. Evid. 404(b); *see also Levy*, 731 F.2d at 1002.

The Second Circuit has adopted an "inclusionary approach" under Rule 404(b) that permits admission of evidence of other crimes, wrongs, or bad acts, unless the evidence is (1) "introduced

for the sole purpose of showing defendant's bad character" or "propensity" to commit crimes, (2) "it is overly prejudicial under Fed. R. Evid. 403," or (3) it is "not relevant under Fed R. Evid. 402." *United States v. Pascarella*, 84 F.3d 61, 69 (2d Cir. 1996) (citations omitted); *Levy*, 731 F.2d at 1002. If evidence is to be admitted under Rule 404(b), an appropriate limiting instruction generally should be issued to the jury if the defendant requests it. *See United States v. Downing*, 297 F.3d 52, 58 (2d Cir. 2002); *United States v. Rutkoske*, 506 F.3d 170, 176-77 (2d Cir. 2007).

B. Argument

1. Griffith's 2018 DPRK Conduct

As is clear from the Background section above, Griffith's trip to the DPRK in April 2019 was a culminating moment in an extensive scheme to provide services to the DPRK and evade sanctions against the DPRK. The scheme began more than a year before the Conference, and continued after the Conference. The Indictment reflects that: Griffith is charged with participating in a conspiracy beginning from "at least in or about August 2018" and continuing until the time of his arrest in November 2019. As the Court has observed, this charge contemplates that "Griffith's speaking engagement at the April 2019 conference was a major step in a long-term plan to persuade and assist the DPRK in using Ethereum to avoid sanctions and launder money." Dkt. 89 at 12. The full scope of Griffith's efforts to provide services to the DPRK, including his discussions and efforts to establish a cryptocurrency mining node in the DPRK beginning in approximately February 2018, therefore constitute direct evidence of the charged sanctions evasion scheme.

Griffith's pursuit of a cryptocurrency mining node in the DPRK, for example, is part of the charged conduct. Griffith's plan to establish the node appears to have commenced in approximately February 2018, but it continued well into at least September 2018 (*i.e.*, into the time period alleged in the Indictment), when Griffith sought a new partner in the Dark Web Entity to bring it to fruition. Intertwined with these efforts, during August and September 2018, Griffith was

also corresponding with CC-1 and CC-2 to pursue traveling to the DPRK in connection with the Conference. Griffith recruited several other co-conspirators who agreed to facilitate his efforts to develop a cryptocurrency node in the DPRK—including CC-3, CC-4, and CC-5—and Griffith continued to collaborate with CC-5 in pursuit of his illicit aims while he was in the DPRK for the Conference, including by contacting CC-5 from the DPRK to place CC-5 in touch with CC-6, a DPRK citizen. Griffith's conduct beginning in 2018 in furtherance of establishing a cryptocurrency mining node in the DPRK, like his conduct at the Conference the following year, is direct evidence of his participation in the charged scheme to provide services to the DPRK and evade applicable sanctions, all in violation of IEEPA. At a minimum, Griffith's actions relating to the DPRK in early 2018 constitute important background evidence to explain and place in context Griffith's steps to contact CC-1 and CC-2, and to ultimately travel to the DPRK to participate in the Conference. Griffith's actions and statements relating to the DPRK during this period are direct evidence necessary to complete the story of the crime charged, and any slight difference in dates from the Indictment is irrelevant. *See United States v. Vasquez*, 133 F.3d 908, 908 (2d Cir. 1998) (unpublished) ("[W]e have repeatedly held that an indictment date only needs to be substantially similar to the date established at trial." (alterations and quotation marks omitted)).

In the alternative, this evidence is admissible pursuant to Rule 404(b) to show, among other things, the defendant's motive, opportunity, intent, preparation, plan, and knowledge. Griffith's efforts to establish a cryptocurrency node in the DPRK, beginning in early 2018, were part of a broader plan to provide services to the DPRK, in violation of the North Korea sanctions regime. *See supra* 26 (NKSR prohibits investing in or providing goods, technology, or services to North Korea). This conduct demonstrates the defendant's preparations to pursue that plan, for example, by developing contacts who could get him access to the DPRK, negotiating the terms of dealing

with the DPRK, and identifying the opportunity for a "lucrative little business" with the DPRK. *See supra* 4.

This conduct also demonstrates that the defendant's motive and intent in traveling to the Conference was not merely to participate in "an opportunity for experts to gather," as the defense has suggested. *See* Dkt. 65 at 10. At trial, the Government anticipates that *mens rea*, and particularly whether the defendant intended to illegally provide a service to the DPRK or DPRK persons, will be a central issue in dispute. When the intent to commit the crime charged is "clearly at issue . . . evidence of prior similar acts may be introduced to prove that intent." *United States v. Mundle*, No. 15 Cr. 315 (NSR), 2016 WL 1071035, at *3 (S.D.N.Y. Mar. 17, 2016) (quoting *United States v. Caputoi*, 808 F.2d 963, 968 (2d Cir. 1987)). Evidence of patterns of evasion of the law are particularly probative where, as here, the Government must prove that the defendant acted willfully. *See United States v. Scali*, 820 F. App'x 23, 27 (2d Cir. 2020) (affirming admission of prior acts pursuant to Rule 404(b) as "circumstantial evidence of willfulness to evade" the law in a tax prosecution) (citing *United States v. Bok*, 156 F.3d 157, 166 (2d Cir. 1998); *United States v. Klausner*, 80 F.3d 55, 63 (2d Cir. 1996)). Griffith's course of conduct in 2018, including his pursuit of the node, is highly probative of whether he subsequently traveled to the DPRK with the intent to provide cryptocurrency-related services to the DPRK in contravention of sanctions. While pursuing the node, the defendant even declared that his plan made "economic sense" precisely because "[i]t'll help them [the DPRK] circumvent the current sanctions on them." These facts demonstrate the defendant's knowledge of the sanctions applicable to the DPRK, as well as his intent to willfully violate them in furtherance of the charged scheme.

2. Griffith's Violation of the DPRK Travel Ban

In the course of Griffith's participation in the charged conspiracy, Griffith committed another crime by willfully and knowingly misusing his U.S. passport in violation of U.S. law.

Specifically, as of September 1, 2017, the U.S. State Department declared that U.S. passports would not be valid for travel to, in, or through North Korea, and that using a U.S. passport for this purpose without receiving a special validation visa from the State Department could constitute a felony, misuse of one's passport, in violation of Title 18, United States Code, Section 1544. Griffith understood this restriction,[11] and sought a special validation visa accordingly, which was unequivocally denied in January 2019. *See supra* 19. Ignoring this denial, Griffith traveled to the DPRK anyway for the Conference in April 2019. Griffith used his U.S. passport to do so, and as he later admitted to law enforcement, he had his DPRK visa issued separately so that it would not appear on his U.S. passport and could be hidden from U.S. authorities. *See supra* 11.

This conduct was inextricably intertwined with Griffith's participation in the charged conspiracy. For example, Griffith and CC-2 communicated explicitly in advance of Griffith's trip about how "the dprk will not stamp your passport" if Griffith elected to travel to the Conference. The relevance of this statement can only be properly understood when placed in context of understanding the U.S.'s prohibitions on travel to the DPRK at the time. Griffith's travel to the DPRK in defiance of U.S. law and the State Department's express disapproval is necessary to complete the story of the crime on trial, and specifically the preparation for and travel to attend the Conference. Griffith's statements to the State Department in pursuit of his travel to the DPRK, including his letter acknowledging the existence of sanctions on the DPRK, only make sense in the context of Griffith's knowledge of the travel prohibition. Moreover, the travel prohibition is relevant to understanding the significance of Griffith's decision to go to the DPRK at all.

[11] As Griffith wrote in a text message on May 2, 2019, after he returned from the Conference, "[i]t's illegal for Americans to visit dprk."

In the alternative, and for similar reasons, the evidence of Griffith's violation of the travel ban is admissible pursuant to Rule 404(b) because it is probative of, among other things, the defendant's intent and knowledge. Particularly in an IEEPA prosecution, where the Government must demonstrate that the defendant acted willfully, Griffith's actions to misuse his passport, defy the U.S. government's tight restrictions on travel to the DPRK, and hide the evidence he had done so, all are highly probative of Griffith's intent to willfully disregard U.S. law in pursuit of the conspiracy. *United States v. Trupin*, 119 F. App'x 323, 326 (2d Cir. 2005) ("[A]ffirmative willful attempt may be inferred from . . . any conduct, the likely effect of which would be to mislead or to conceal." (quoting *Spies v. United States*, 317 U.S. 492, 499 (1943))). Griffith traveled to the DPRK in the face of the U.S. government's clear and strong directive that even such travel on a U.S. passport constituted a crime. Evidence of Griffith's violation of that rule, during the course of the charged crime and in furtherance of that crime, is plainly relevant to show Griffith's state of mind and has substantial probative value.

3. Griffith's Post-Conference Conduct

Griffith's post-Conference efforts to provide services to the DPRK, including by attempting to facilitate a financial transaction of 1 ether with the DPRK,[12] assisting in the promotion of a second cryptocurrency conference to be held in the DPRK in 2020, recruiting others in the cryptocurrency industry to travel to the DPRK, attempting to fund travel for DPRK persons to work with a technology association, and monetizing DPRK domain names are also direct evidence of the charge in this case. All of this conduct occurred within the time period charged in the Indictment, specifically the months following the Conference and leading up to the defendant's

[12] As of July 29, 2021, the value of a single ether was equivalent to approximately $2,337.59 U.S. dollars.

arrest. This conduct was also well within the scope of the conspiracy's dual aims to provide services to the DPRK, and to evade and avoid the requirements of U.S. law with respect to the provision of services to the DPRK. Each of these actions, had they succeeded, would have provided "useful labor or human effort" to the DPRK, and in the case of the contemplated 1 ether exchange and travel funding, an explicit financial transaction service. *See* Dkt. 89 at 9-10 (defining the term "service"). Griffith's plans to acquire DPRK internet domain names, and to potentially aid the DPRK to auction them off as "assets" in exchange for value, similarly presented another avenue for providing services, and even direct funding, to the DPRK. Promoting a second conference and recruiting others with cryptocurrency expertise to travel to the DPRK, in order to provide lessons to DPRK persons, is likewise a marketing, advertising, or brokering service that was part and parcel of Griffith's contributions to the conspiracy. *See, e.g.*, *supra* 5 (noting that Griffith's own company attempted to hire an outside vendor to perform services that included "[s]eeking for and introducing potential business partners or personnel to the Company").

In the alternative, evidence of the defendant's post-Conference conduct is also admissible pursuant to Rule 404(b) to prove, among other things, the defendant's motive, intent, preparation, plan, knowledge, and absence of mistake or accident. Griffith's actions during this period are particularly probative of Griffith's intent to violate sanctions, his knowledge that his actions would violate sanctions, and his plan and preparation to commit the charged crime in the face of that knowledge, because Griffith pursued these actions even after the FBI expressly advised him that his conduct would likely violate IEEPA. *Germosen*, 139 F.3d at 128 (holding that "'[s]ubsequent act' evidence may be admitted under Rule 404(b)," and affirming admission of such evidence where it was "directly relevant to [the defendant's] claimed lack of intent" in the charged conspiracy). The FBI provided Griffith this admonishment precisely because Griffith admitted to

them that he was interested in returning to the DPRK, and in facilitating cryptocurrency exchanges with the DPRK. Evidence of Griffith's conduct during this period is similarly admissible, both as direct evidence and pursuant to Rule 404(b), to demonstrate that Griffith remained a willful member of the charged conspiracy even after he purported to self-report his conduct to the FBI.

4. Griffith's Statements About Money Laundering, U.S. Citizenship, and the Payment of Taxes

Griffith's statements during the course of the offense and within the charged time period about setting up a money laundering company in North Korea, regarding his interest in renouncing his U.S. citizenship and purchasing citizenship elsewhere in the wake of his contacts with the FBI, and about his failure to pay taxes are also part of the direct evidence of the charged conduct in this case and, alternatively, are admissible under Rule 404(b).

As described above, 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." Later, in the wake of Griffith's first interview with the FBI, 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."

In addition, immediately after his first FBI interview in May 2019, Individual-5 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." 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." 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."

These statements constitute direct evidence. Griffith's proclamation that he would set up a money laundering company is direct proof that he intended to continue to assist the DPRK and that he sought, or at least believed it possible, to use his newfound DPRK connections to further advance the objective of providing illicit services to the DPRK. Griffith's statements about renouncing his U.S. citizenship shortly after speaking with FBI is evidence that Griffith considered severing his ties to the United States to avoid additional law enforcement scrutiny that could hinder him in continuing to pursue the objective of providing services to and doing prospective business with the DPRK.

Griffith's statements about his taxes, and what other conduct the FBI might be interested in, are also direct evidence. Griffith's acknowledgement, in response to being advised to get his taxes in order, that the FBI already "have plenty to get me with" even "[w]ithout any taxes" as a result of his "[v]isiting dprk," and that he could be imprisoned for ten years for traveling to the DPRK," constitute admissions of conduct directly relevant to and part of the charged crime, including his travel to the DPRK to participate in the Conference. Additionally, Griffith's later statements that he had not filed taxes constitute direct evidence of his ongoing participation in the charged conspiracy to provide services to the DPRK and evade U.S. law with respect to the provision of such services. Griffith made those statements during the charged time period and in the context of having been warned that the FBI would be interested in tax non-compliance as it

investigated him for his DPRK-related activities. Griffith's admission that although he had not filed taxes he was prepared to lie about doing so, evidences that Griffith wanted to deceive the FBI agents investigating him about this case and believed that he needed to do so to avoid further scrutiny from law enforcement relating to his provision of services to the DPRK. In other words, Griffith's statements about his taxes are direct evidence of his efforts to evade law enforcement detection in furtherance of his continuing participation in the ongoing scheme to assist the DPRK.

In addition, evidence of the defendant's statements regarding these topics is also admissible pursuant to Rule 404(b) to show, among other things, the defendant's motive, intent, plan, preparation, knowledge, and absence of mistake or accident. Griffith's statement that he could "set[] up a money laundering company in North Korea," for example, reflects his intent, knowledge, and absence of any mistake with respect to his dealings in the DPRK, the possible uses for his services, and his value to the DPRK. In addition, Griffith's statements about his U.S. citizenship, including that he needed a second passport following his meeting with the FBI, reflects his intent and plan to potentially flee the U.S. rather than face the consequences for his actions before the U.S. justice system. Griffith's conversations about his tax non-compliance evidence Griffith's plan to deceive the FBI agents investigating him for his DPRK-rleated activities, which is highly probative of Griffith's knowledge, intent, and absence of mistake in engaging in those activities in violation of sanctions. These statements also demonstrate Griffith's guilty conscience in light of his criminal conduct. Particularly where, as here, the Government must prove willfulness and *mens rea* will be squarely at issue at trial, the statements described above, which are probative of the defendant's state of mind and whether he knowingly acted unlawfully in seeking to provide services to the DPRK, are admissible pursuant to Rule 404(b). *See United States v. Zackson*, 12 F.3d 1178, 1182 (2d Cir. 1993) (where a defendant claims that his conduct has an innocent

explanation, other act evidence is generally admissible to prove that the defendant acted with the state of mind necessary to commit the offense charged); *United States v. Dupree*, 870 F.3d 62, 76 (2d Cir. 2017) (a court may "admit evidence of prior acts as probative of knowledge and intent if the evidence is relevant to the charged offense, i.e., if there is a similarity or connection between the charged and uncharged acts").

5. The Evidence Satisfies Rule 403

Finally, the proposed evidence satisfies Rule 403. None of the evidence outlined above is unduly prejudicial relative to other proof the Government expects to offer. The proof at trial will include recordings of Griffith's own conduct and that of his co-conspirators, caught in the act of providing services to the DPRK and DPRK persons. It will also include Griffith's statements expressing minimal regard for the consequences of his actions, even if they contributed to the DPRK's nuclear weapons program, *see supra* 7, and Griffith's own notes of his activities in the DPRK, which included firing guns used to kill Americans and touring a captured U.S. battleship. Evidence is not unduly prejudicial when it is not "more inflammatory than the charged crime." *United States v. Livoti*, 196 F.3d 322, 326 (2d Cir. 1999); *United States v. Pitre*, 960 F.2d 1112, 1120 (2d Cir. 1992); *United States v. Roldan Zapata*, 916 F.2d 795, 804 (2d Cir. 1990). Accordingly, evidence of the full scope of Griffith's efforts to provide services to the DPRK, Griffith's violation of the U.S. prohibitions on travel to the DPRK, and Griffith's other statements reflecting his disregard for U.S. law and U.S. authorities is not barred by Rule 403. Moreover, any risk of undue prejudice could be addressed through an appropriately crafted jury instruction. *See Zackson*, 12 F.3d at 1182; *Livoti*, 196 F.3d at 326.

II. Statements of Griffith's Co-Conspirators Are Admissible

At trial, the Government will offer statements of the co-conspirators identified in the Background section above. These statements are admissible as co-conspirator statements, pursuant

to Rule 801(d)(2)(E), and as statements against interest, pursuant to Rule 804(b)(3). As described above, the Government's proof of these statements will come almost entirely from Griffith's digital devices and electronic accounts—the statements were made in the course of communications between the co-conspirators directly with Griffith during the conspiracy, and will be offered in conjunction with Griffith's plainly admissible statements from those exchanges—from recordings of the Conference, or Griffith's own interviews with FBI.

A. Applicable Law

1. Rule 801(d)(2)(E): Co-Conspirator Statements

Rule 801(d)(2)(E) of the Federal Rules of Evidence provides in relevant part, "A statement is not hearsay if . . . the statement is offered against an opposing party and was made by the party's co-conspirator during and in furtherance of the conspiracy." To admit a statement pursuant to this Rule, the Court must find two facts by a preponderance of the evidence: *first*, that a conspiracy that included the declarant and the defendant existed; and *second*, that the statement was made during the course and in furtherance of that conspiracy. *Bourjaily v. United States*, 483 U.S. 171, 175 (1987).

Once a conspiracy is shown to exist, the "evidence sufficient to link another defendant to it need not be overwhelming," and "the 'in furtherance' requirement of Rule 801(d)(2)(E) is satisfied" when, for example, "a co-conspirator is apprised of the progress of the conspiracy, or when the statements are designed to induce his assistance." *United States v. Paone*, 782 F.2d 386, 390 (2d Cir. 1986) (internal quotation marks omitted). Statements between co-conspirators that "provide reassurance, serve to maintain trust and cohesiveness among them, or inform each other of the current status of the conspiracy," further the conspiracy, *United States v. Simmons*, 923 F.2d 934, 945 (2d Cir. 1988), as do statements "that apprise a co-conspirator of the progress of the conspiracy," *United States v. Rahme*, 813 F.2d 31, 36 (2d Cir. 1987).

2. Rule 804(b)(3): Statements Against Interest

Under Rule 804, if a declarant is "unavailable," there is an exception to the hearsay rule where:

> (A) a reasonable person in the declarant's position would have made [the statement] only if the person believed it to be true because, when made, it was so contrary to the declarant's proprietary or pecuniary interest or had so great a tendency to invalidate the declarant's claim against someone else or to expose the declarant to civil or criminal liability; and
>
> (B) is supported by corroborating circumstances that clearly indicate its trustworthiness, if it is offered in a criminal case as one that tends to expose the declarant to criminal liability.

Fed. R. Evid. 804(b)(3). This rule "is founded on the commonsense notion that reasonable people, even reasonable people who are not especially honest, tend not to make self-inculpatory statements unless they believe them to be true." *Williamson v. United States*, 512 U.S. 594, 599 (1994).

To satisfy Rule 804(b)(3), the proponent of the statement must show by a preponderance of the evidence: "(1) that the declarant is unavailable as a witness, (2) that the statement is sufficiently reliable to warrant an inference that a reasonable man in [the declarant's] position would not have made the statement unless he believed it to be true, and (3) that corroborating circumstances clearly indicate the trustworthiness of the statement." *United States v. Wexler*, 522 F.3d 194, 202 (2d Cir. 2008) (internal quotation marks omitted). A declarant is unavailable for purposes of Rule 804 if, as relevant here, the declarant is "exempted from testifying about the subject matter of the declarant's statement because the court rules that a privilege applies," Fed. R. Evid. 804(a)(1), or "is absent from the trial or hearing and the statement's proponent has not been able, by process or other reasonable means, to procure the declarant's attendance or testimony," *id.* 804(a)(5)(B).

"A statement will satisfy Rule 804(b)(3)'s requirement that it 'tended' to subject the declarant to criminal liability if it would be probative in a trial against the declarant." *United States*

v. Persico, 645 F.3d 85, 102 (2d Cir. 2011) (internal quotation marks omitted). Moreover, a declarant need not "be aware that the incriminating statement subjects him to immediate criminal prosecution," but instead, that the "incriminating statement sufficiently tended to subject the declarant to criminal liability so that a reasonable man in his position would not have made the statement unless he believed it to be true." *United States v. Lang*, 589 F.2d 92, 97 (2d Cir. 1978) (internal quotation marks and citation omitted).

Finally, the Second Circuit requires corroboration of both the declarant's and the statement's trustworthiness. *United States v. Doyle*, 130 F.3d 523, 543-44 (2d Cir. 1997). Statements made to co-conspirators, not in response to questioning, and not made in coercive atmospheres are sufficiently reliable for purposes of this Rule. *See, e.g.*, *United States v. Matthews*, 20 F.3d 538, 546 (2d Cir. 1994).

B. Discussion

The statements of CC-1, CC-2, CC-3, CC-4, CC-5, and CC-6, including those described above, are admissible as co-conspirator statements and as statements against interest.

As described above, CC-1 and CC-2 were organizers of the Conference who conspired with Griffith to commit the charged offense by, among other things, facilitating Griffith's travel to North Korea and Griffith's acting as a keynote speaker at the Conference. CC-1's above-described statements were in furtherance of the conspiracy, including, for example, his emails explaining how Griffith could secure a visa to the DPRK by sending an email and materials to the DPRK UN Mission in Manhattan. *See supra* 10. CC-2's statements were similarly made in furtherance of the conspiracy, including his presentation at the Conference, alongside Griffith, about how the North Korean attendees could avoid sanctions by using an "OTC provider." *See supra* 15.

Griffith also brought CC-3, CC-4, and CC-5 into the conspiracy to provide services to the DPRK. These individuals acted as facilitators, whom Griffith identified as having the ability to assist Griffith to further his goals of helping the DPRK to set up an Ethereum node inside North Korea and later to arrange for the DPRK to conduct a 1 ether cryptocurrency transaction with South Korea. Their statements, including those above, were also in furtherance of the conspiracy, including CC-3's correspondence connecting Griffith with CC-4, *see supra* 3, CC-4's confirmation that he held "many meetings" and was "in talks with [North] Koreans at the Internet company in Pyongyang who will be able to get this node online for you," *see supra* 5, and CC-5's statement that "the NK [North Korea] node idea was considered" by a North Korean company, *see supra* 5.

Similarly, CC-6 was the North Korean "minder" that acted as Griffith's guide and assigned government representative in North Korea and to whom Griffith wrote emails after the Conference, as part of Griffith's continuing efforts to provide services to the DPRK. CC-6 also made statements in furtherance of the conspiracy, including when Griffith facilitated a video call with CC-5 to discuss the 1 ether cryptocurrency transaction. *See supra* 17.

The above-described statements of the six referenced co-conspirators are also admissible under Rule 804(b)(3). Each of these co-conspirators are presently unavailable because they are citizens of countries other than the United States and reside outside the United States. *See United States v. Ortiz*, 962 F. Supp. 2d 565, 573 (S.D.N.Y. 2013) (finding witness unavailable where located outside United States at time of trial). In addition, each is currently likely to invoke the Fifth Amendment if they were questioned under oath regarding these activities. *See United States v. Savoca*, 335 F. Supp. 2d 385, 390 (S.D.N.Y. 2004) ("[T]he 'unavailability' component is established by the fact that [the declarant] is expected to invoke his Fifth Amendment privilege.").

Each of the co-conspirators' statements were made in the context of helping to further Griffith's unlawful provision of services to the DPRK as well as the scheme to evade and avoid U.S. sanctions outlawing the provision of services by U.S. citizens to DPRK persons. These statements, therefore, "implicated [the declarants] in [illegal] activity," and each declarant "would not have made the statement unless he believed it to be true." *Dupree*, 870 F.3d at 80; *see also Ortiz*, 962 F. Supp. 2d at 573. In addition, the statements are sufficiently reliable because they were made in confidence with the defendant, or to persons inside the DPRK, "whom the declarant[s] believe[d] [were] all[ies], not . . . law enforcement official[s]." *United States v. Sasso*, 59 F.3d 341, 349 (2d Cir. 1995).

III. Statements by Individuals Not Alleged to be Co-Conspirators that Are Necessary to Understand Griffith's Statements Are Admissible for that Non-Hearsay Purpose

The statements of Individual-1, Individual-2, Individual-3, Individual-4, and Individual-5 (the "Individuals") described in the Background section above are also admissible. While the Government is not alleging that these Individuals joined the charged conspiracy, Griffith made statements to them that are admissible and probative of his criminal conduct. The Government intends to offer these Individuals' statements, which were made in the course of direct correspondence with Griffith, not for the truth of the matter asserted, but for the limited purpose of placing Griffith's plainly admissible statements in context and enabling the jury to understand those statements.

As an initial matter, many of these statements are questions, instructions, or proposals. *See, e.g.*, *supra* 7 (Individual-3 asked why Griffith was willing to risk his safety to go to a conference in the DPRK?), 21 (Individual-5 asked "What do you hope to gain from your second visit?"). Such statements are categorically not hearsay because such statements are not offered for the truth. *See United States v. Bellomo*, 176 F.3d 580, 586 (2d Cir. 1999) ("Statements offered as evidence of

commands or threats or rules directed to the witness, rather than for the truth of the matter asserted therein, are not hearsay."); *Fischl v. Armitage*, 128 F.3d 50, 58 (2d Cir. 1997) (holding that "instructions" issued by one member of a conspiracy to another are not hearsay under Rule 801(c)); *United States v. Oguns*, 921 F.2d 442, 449 (2d Cir. 1990) ("An inquiry is not an 'assertion,' and accordingly is not and cannot be a hearsay statement." (internal quotation marks omitted)).

To the extent that the Individuals' statements are not covered by the aforementioned categories of non-hearsay, the Government seeks to offer such statements for the limited purpose of placing Griffith's statements in context and not for the truth of any matters asserted. *See, e.g.*, *supra* 9 (Individual-4 told Griffith "[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" and warned Griffith not to discuss "anything that helps circumvent sanctions," to which Griffith responded with a thumbs up emoji and, "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.'"), 22 (Individual-5 told Griffith "It makes me nervous for you to defy the government and go again" to which Griffith responded "I'll figure something out . . . Worst comes to worst I'll send an emissary."). It is well settled that statements of witnesses not appearing at trial are properly admitted for this limited purpose. *See United States v. Barone*, 913 F.2d 46, 49 (2d Cir. 1990) (upholding admission of statements of "informant who is heard in a tape-recorded conversation with the defendant[,] [s]o long as the informant's recorded statements are not presented for the truth of the matter asserted, but only to establish a context for the recorded statements of the accused . . . ."); *see also United States v. McNair*, 46 F. App'x 658, 659-60 (2d Cir. 2002) (summary order) (upholding admission of recordings between defendant and non-testifying

informant where informant's statements "were not offered to prove the truth of the matters asserted but only to render what [the defendant] said in these conversations intelligible" (internal quotation marks omitted) (citing *United States v. Sorrentino*, 72 F.3d 294, 298 (2d Cir. 1995)); *United States v. Romano*, No. 12 Cr. 691 (JFK), 2014 WL 69794, at *1 (E.D.N.Y. Jan. 8, 2014) (same); *United States v. Walker*, No. 99 Cr. 379 (BSJ), 1999 WL 777885, at *4 (S.D.N.Y. Sept. 29, 1999) (same).

IV. Extraneous Evidence Regarding the DPRK's Alleged Cryptocurrency Capabilities Should Be Precluded

Extraneous evidence regarding the DPRK's alleged cryptocurrency and blockchain capabilities should be precluded because it is not relevant and would be likely to confuse the jury. *See* Fed. R. Evid. 401, 403. For example, the defense has suggested to the Government that they will seek to introduce evidence to show that the DPRK government allegedly sponsored hacking and theft relating to cryptocurrency on other occasions, wholly unrelated to the events of this case, the members of the charged conspiracy, or the attendees of the Conference. The defense has signaled that they intend to seek to use such evidence to draw broad purported inferences about the DPRK's alleged capabilities prior to Griffith's involvement. As discussed in greater detail below, the Government agreed to be bound by a stipulation regarding these matters in order to take this issue out of the case. In light of this stipulation, the defense should be similarly prevented from offering this irrelevant and speculative evidence, which has no bearing on the existence of the charged conspiracy or whether the defendant participated in it, and would be likely to confuse, distract, and mislead the jury.

A. Relevant Background

During pretrial litigation, Griffith moved to compel a wide-ranging search across multiple agencies of the U.S. government for "documents and communications regarding the U.S. government's knowledge and analysis of the DPRK's blockchain and cryptocurrency

capabilities." Dkt. 63 at 14. Through this motion, Griffith signaled that he intended to argue at trial that he did not conspire to perform a service because "the scope of information on cryptocurrency and blockchains [presented at the Conference was] already in the DPRK's possession and/or more widely in the public domain." *Id.* at 15. Following extensive colloquy at multiple conferences and submissions from the parties, the Court denied Griffith's motion to compel as moot after the Government agreed to the following stipulation (the "Stipulation"):

> The Government will not present argument or evidence that the information that Mr. Griffith allegedly provided and intended to provide while in North Korea for the Cryptocurrency Conference in April 2019 was beyond the then-existing capabilities and knowledge of the government of the Democratic People's Republic of Korea, but may present evidence that certain individuals at the Conference gained information new to them.

Dkt. 99 at 1. The Government noted that its agreement to the Stipulation was predicated on its understanding that the Stipulation would not foreclose the Government from introducing otherwise admissible evidence, subject to any appropriate limiting instruction, of the defendant's statements, co-conspirator statements, or events at the Conference. *See* Dkt. 96, citing Feb. 23, 2021 Tr. at 16-19; *id*. at 4-5 (discussing examples of this type of evidence). For example, the evidence that the Government will offer at trial includes that Griffith told FBI about the lack of sophistication of those attending the Conference and stated that the DPRK could not build a cryptocurrency without China's assistance, see supra 20, and Griffith's statement to Individual-3 that the DPRK would "probably like to start" to "fund . . . their drug trade and nuclear program with crypto," *see supra* 7.

B. Applicable Law

The Federal Rules of Evidence define relevant evidence as evidence that "has any tendency to make a fact more or less probable than it would be without the evidence; and . . . the fact is of consequence in determining the action." Fed. R. Evid. 401. Irrelevant evidence is not admissible.

Fed. R. Evid. 402. Even the admissibility of relevant evidence has its limits. Courts may exclude relevant evidence where its probative value is substantially outweighed by a danger of prejudice, confusion of the issues, wasting time, or needlessly presenting cumulative evidence. Fed. R. Evid. 403.

These fundamental principles apply to both parties in a criminal prosecution. "[P]roperly applied evidentiary rules that serve legitimate interests in the criminal trial process, and the resulting restrictions on the presentation of evidence [are] neither arbitrary nor disproportionate to those purposes." *United States v. Stewart*, 433 F.3d 273, 312 (2d Cir. 2006) (internal citations and quotation marks omitted) (upholding preclusion of evidence proffered by the defense). A defendant's "wide-ranging right to present a defense" still "does not give him a right to present irrelevant evidence." *See United States v. Maxwell*, 254 F.3d 21, 26 (1st Cir. 2001) (internal citations omitted).

C. Argument

Extraneous evidence regarding the DPRK government's purported cryptocurrency capabilities and knowledge should be precluded as irrelevant to the charged conduct.

Whether or not and to what extent individuals or components within the DPRK government possessed the independent capability to perform a given action at any moment in time, or to obtain a given service from someone other than the defendant, is not relevant to whether the defendant committed the crime charged in the Indictment. The Government has not alleged, and need not prove at trial, that the services Griffith conspired to provide were uniquely his to give, or were necessarily outside the capabilities of certain individuals or entities within the DPRK, in order to constitute services under the NKSR. Under the NKSR, a "service" may be an act done for the benefit or at the command of another, the performance of work commanded or paid for by another, or any other useful labor or human effort, whether or not compensation for that service was

contemplated,[13] and includes performing advocacy in coordination with, or at the direction of, another,[14] or facilitating the transfer of funds on behalf of another person or entity.[15]

To convict Griffith on the sole count of the Indictment, the Government must prove only that the defendant willfully agreed with others to provide services to the DPRK or DPRK persons without obtaining a license, or to evade and avoid sanctions against North Korea with respect to the provision of such services, or to attempt to do so. Even if, solely for the sake of argument, the DPRK was already capable of doing the things that Griffith conspired to do, Griffith's provision of that service would still violate IEEPA. As explained in detail above, Griffith conspired to and did provide a service to the DPRK and the North Korean Conference attendees in multiple ways, by seeking to develop cryptocurrency infrastructure and equipment inside North Korea, presenting at the Conference, teaching North Koreans how to evade and avoid U.S. sanctions through cryptocurrency transactions, developing plans to create specialized "smart contracts" for the DPRK, and brokering introductions for the DPRK to other cryptocurrency service providers. *See, e.g.*, *Banki*, 685 F.3d at 108 (stating that the Iranian sanctions "prohibit the exportation of not only advice on developing Iranian chemical weapons but also advice on developing Iranian petroleum resources, *see* § 560.209; not only services to the Iranian government but also services to Iranian businesses, *see* § 560.204; and not only bombs but also beer, *see* § 560.204"). Nor was Griffith's

[13] *See* Dkt. 89 at 9-10, citing Merriam–Webster's Collegiate Dictionary 1067 (a service is "useful labor that does not produce a tangible commodity"); Black's Law Dictionary 1372 (7th ed. 1999) (a service is an "intangible commodity in the form of human effort"); *Holder v. Humanitarian Law Project*, 561 U.S. 1, 23-24 (2010) (defining "service," consistent with *Banki*, to mean "the performance of work commanded *or* paid for by another" or "an act done for the benefit or at the command of another").

[14] *Holder v. Humanitarian Law Project*, 561 U.S. at 24 (finding that "a person of ordinary intelligence would understand the term 'service' to cover advocacy performed in coordination with, or at the direction of, a foreign terrorist organization").

[15] *United States v. Banki*, 685 F.3d 99, 107–08 (2d Cir. 2012), as amended (Feb. 22, 2012).

conduct limited to merely imparting basic, previously published information at the Conference as the defense has claimed. Moreover, the Stipulation precludes the Government from placing at issue whether Griffith's services were "beyond the then-existing capabilities and knowledge of the government of the Democratic People's Republic of Korea," thereby eliminating any need for the defense to purport to meet such evidence.

Notably, Griffith is charged with conspiring to provide a service to the DPRK, not with providing "technology" to the DPRK, which is a separate prohibition in the NKSR. *See supra* 26. While the evidence overwhelmingly indicates that Griffith violated this prohibition as well, the jury need not determine whether or not Griffith's presentation or other conduct amounted to a transfer of technology or any technological advancement to the DPRK.

Even if individuals within the DPRK or its government did have certain cryptocurrency capabilities, those facts do not bear on whether Griffith and his co-conspirators agreed to offer and provide services to the DPRK, such that Griffith is guilty of the charged offense. Moreover, Griffith's statements in the course of the conspiracy consistently reflect that he believed he was providing new technology and services to the DPRK and the DPRK audience at the Conference.

The inchoate nature of the charged offense further underscores the irrelevance of the information that should be precluded consistent with the Stipulation. The Government need not prove that Griffith's services were in fact helpful to the government of the DPRK, or even any individual attending the conference, so long as Griffith agreed with others and intended to provide a service, to evade or avoid sanctions. The conspiracy need not have succeeded in providing the DPRK with a service, let alone one that was demonstrably helpful to the DPRK. Griffith had no way knowing precisely what the DPRK or all of the individual Conference attendees knew about blockchain and cryptocurrency technologies. To the contrary, Griffith told the FBI that he believed

that he introduced new concepts to the North Korean Conference attendees, and that the attendees left with a better understanding of blockchain and cryptocurrency technologies. And as Griffith told the Conference attendees, "the technology is still fairly new . . . [s]o . . . 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."

In addition, any possible probative value of extraneous evidence about the DPRK's alleged cryptocurrency and blockchain capabilities would be far outweighed by the risk that such evidence would confuse or mislead the jury, including by improperly suggesting that the jury must determine what the cryptocurrency and blockchain capabilities of the DPRK government were in order to assess the charge against the defendant. *See* Fed. R. Evid. 403. In other words, such testimony would tend to suggest to the jury that the jury must consider whether any service encompassed by the conspiracy could not constitute a service at all because it involved only capabilities that the DPRK already knew how to perform on its own. This is not part of the elements of the crime, and would mislead the jury as to the applicable law. Indeed, this line of argument would present the jury with an incorrect and unduly narrow conception of "services," as reflected in the above discussion of the applicable definition of that term in the sanctions regulations. Presenting such evidence and argument to the jury would be highly likely to create confusion, distract from the relevant issues, and invite speculation. Any conceivable probative value for this evidence would be substantially outweighed by a danger of confusing the issues, misleading the jury, and wasting time on a distracting sideshow, particularly where the Stipulation has already taken this matter out of the Government's case, such that the defense should also not be permitted to introduce such extraneous and irrelevant evidence. *See Beastie Boys v. Monster Energy Co.*, 983 F. Supp. 2d 369, 375 (S.D.N.Y. 2014) (noting "paridigmatic concern" under Rule 403 of "an

orderly proceeding's being derailed by a 'trial within a trial'"); *see, e.g.*, *United States v. Aboumoussallem*, 726 F.2d 906, 910-13 (2d Cir. 1984) (precluding defendant from introducing evidence where such evidence was likely to lead to a "trial within a trial" and jury confusion); *United States v. Al Kassar*, 582 F. Supp. 2d 498, 500 (S.D.N.Y. 2008), *aff'd*, 660 F.3d 108, 123-24 (2d Cir. 2011) (same). Extraneous evidence of the DPRK's alleged cryptocurrency and blockchain capabilities should therefore be precluded at trial.

CONCLUSION

For the reasons set forth herein, the Court should grant the Government's motions *in limine*.

DATED: New York, New York
August 13, 2021

Respectfully submitted,

AUDREY STRAUSS
United States Attorney
Southern District of New York

By: /s/
Kimberly J. Ravener
Kyle A. Wirshba
Assistant United States Attorneys
Tel: (212) 637-2358 / 2493