UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,	:	
– against –	:	**MEMORANDUM DECISION AND ORDER**
HUAWEI TECHNOLOGIES CO., LTD., *et al.*,	:	18-CR-457 (S-3) (AMD) (CLP)
Defendants.	:	

ANN M. DONNELLY, United States District Judge:

Before the Court is the defendants'[1] motion to dismiss all but three counts of the sixteen count third superseding indictment. (ECF Nos. 474, 475.) As explained below, the motion is denied.

BACKGROUND

I. Factual Background

The 55-page third superseding indictment, which includes a lengthy factual description, charges the defendants with racketeering conspiracy, in violation of 18 U.S.C. § 1962(d); conspiracy to steal trade secrets, in violation 18 U.S.C. § 1832(5); wire fraud and wire fraud conspiracy, in violation of 18 U.S.C. §§ 1343 and 1349; bank fraud and bank fraud conspiracy, in violation of 18 U.S.C. §§ 1344 and 1349; conspiracy to defraud the United States, in violation of 18 U.S.C. § 371; conspiracy to violate and violations of the International Emergency Economic Powers Act ("IEEPA"), in violation of 50 U.S.C. § 1705(a); money laundering conspiracy, in violation of 18 U.S.C. § 1956(h); and conspiracy to obstruct justice, in violation of

[1] The moving defendants are Huawei Technologies Co, Ltd. ("Huawei"), Huawei Device Co., Ltd. ("Huawei Device"), Huawei Device USA, Inc. ("Huawei Device USA"), and Futurewei Technologies, Inc. ("Futurewei"). Unless otherwise specified, the term "defendants" refers to these four entities.

18 U.S.C. 1512(k). (ECF No. 126.) According to the allegations in the indictment, which "the Court must treat . . . as true," *United States v. Coffey*, 361 F. Supp. 2d 102, 111 (E.D.N.Y. 2005); *see also United States v. Goldberg*, 756 F.2d 949, 950 (2d Cir. 1985), the defendants, over the course of years, participated in schemes to misappropriate intellectual property, defraud financial institutions and obstruct justice.

a. Misappropriation of Intellectual Property

According to the indictment, from 2000 to 2018, the defendants "executed a scheme to operate and grow the worldwide business" of Huawei "through the deliberate and repeated misappropriation of intellectual property" of companies headquartered or operating in the United States. (ECF No. 126 ¶ 8.) In furtherance of this scheme, the defendants "entered into . . . and then violated the terms of . . . confidentiality agreements" with competitor companies, tried to recruit competitor companies' employees "to gain access to intellectual property of their former employers," and "used proxies such as professors working at research institutions or third party companies" to access "nonpublic intellectual property." (*Id.* ¶¶ 11–12.) Huawei also encouraged its employees to steal intellectual property from other companies by "launch[ing] a formal policy instituting a bonus program to reward employees who obtained confidential information from competitors." (*Id.* ¶ 11, 13.) The indictment alleges that the defendants obstructed civil and criminal proceedings related to the misappropriation of intellectual property by providing "false information in the form of affidavits or reports of internal investigations" and "instruct[ing] employees to conceal information from law enforcement." (*Id.* ¶ 14.)

The indictment identifies six companies from which the defendants misappropriated intellectual property.

i. Company 1

Beginning in 2000, Huawei and Futurewei stole copyrighted "operating system source code for internet routers, command line interface . . . and operating system manuals" from Company 1, an American technology company headquartered in California. (*Id.* ¶ 18.) From April through December 2002, Huawei incorporated this source code into internet routers that Futurewei marketed as cheaper versions of Company 1's routers and sold in the United States. (*Id.* ¶¶ 18–19.) In furtherance of this scheme, Huawei and Futurewei "hired or attempted to hire Company 1 employees and directed these employees to misappropriate Company 1 source code." (*Id.* ¶ 18.)

In December 2002, representatives of Company 1 "notified senior [Huawei] executives . . . of the misappropriation." (*Id.* ¶ 20.) Huawei and Futurewei "agreed to replace the original versions of some of the misappropriated source code" and to "recall from the U.S. market products that included the misappropriated source code." (*Id.*)

In 2003, Company 1 sued Huawei and Futurewei in a Texas federal court for intellectual property infringement. (*Id.* ¶ 21.) Although Huawei and Futurewei claimed that they had removed the stolen source code from their products, they in fact destroyed evidence by erasing the memory drives of recalled routers, sending those routers to China, and by trying to erase stolen source code on sold routers by getting remote access to them. (*Id.*) To minimize their damages and to make it appear that they did not misappropriate the source code, a Huawei executive filed a false declaration claiming that a third party gave Huawei Company 1's source code. (*Id.* ¶ 22.) Finally, a neutral examiner, on whom the parties agreed, compared Company 1's source code with Huawei's source code and concluded that certain portions were "substantially similar to or developed or derived from Company 1's source code" and had been misappropriated. (*Id.* ¶ 23.)

i. Company 2

Between 2000 and 2003, Huawei recruited an engineer employed by Company 2, an American technology company headquartered in Illinois, to misappropriate Company 2's intellectual property. (*Id*. ¶¶ 25–26.)[2] Huawei executives met with the engineer "multiple times" in China. (*Id.* ¶ 26.) After a February 2003 meeting, the engineer emailed a Huawei employee a confidential "50-page document with technical specifications for a base station, designed for use in wireless network, manufactured by Company 2." (*Id.* ¶ 27.)

i. Company 3

During a July 2004 trade show in Chicago, a Huawei employee was discovered "removing the cover from . . . and taking photographs of the circuitry" of Company 3's networking device. (*Id.* ¶ 28.) Huawei wanted to steal the technology so that it could "save on research and development costs in the development of its own networking device." (*Id.* ¶ 29.) Huawei claimed to Company 3 that the employee was a "junior engineer" who had never been to the United States, that he "attended the trade show in his personal capacity," that he acted "without Huawei's authorization," and that his "actions do not reflect to culture or values of Huawei." (*Id.* ¶ 28.)[3]

i. Company 4

Company 4 operated in California and New York. (*Id.* ¶ 30.) In 2009, Huawei and Futurewei "devised a scheme to misappropriate [Company 4's] technology related to antennas that provide cellular telephone and data services." (*Id.*) Huawei and Futurewei executed this

[2] Internal Huawei emails discuss meeting with the engineer in China and Huawei's plans to recruit him establish that Huawei targeted the engineer "[n]o later than October 2001." (*Id.* ¶ 26.)

[3] In 2012, the employee "submitted" a resume to the United States government in which he stated that he was a "senior R&D Engineer" at Huawei from 1997 to 2004. (*Id.*)

scheme by feigning an interest in forming a partnership with Company 4. (*Id.* ¶¶ 31–33.) As part of that endeavor, Futurewei signed a non-disclosure agreement that prevented it from using Company 4's confidential information "for [Futurewei's] own benefit or the competitive disadvantage of Company 4." (*Id.* ¶ 31.)

On September 21, 2009, Company 4 gave a slide presentation to Huawei about its proprietary technology, a trade secret. (*Id.* ¶ 32.) Each slide was marked "Commercial in Confidence." (*Id.*) The same day, a Huawei employee emailed a Futurewei engineer "expressing interest" in Company 4's technology. (*Id*. ¶ 33.) On October 23 and 26, 2009, the Futurewei engineer emailed his colleagues about his ideas for implementing Company 4's technology. (*Id.*) On October 30, 2009, Futurewei filed a provisional patent application that "used and relied in large part upon the Company 4 intellectual property." (*Id.*) Between 2009 and 2016, Huawei received about $22 million from the sale of products that used Company 4's intellectual property. (*Id.* ¶ 34.)

i. Company 5

Beginning in 2012, Huawei, Huawei Device, and Huawei Device USA "devised a scheme to misappropriate robot technology" from Company 5, an American wireless network operator headquartered in Washington. (*Id.* ¶ 35.) Huawei Device wanted "to save on research and development costs." (*Id.* ¶ 44.) Huawei Device's "efforts to obstruct civil litigation with Company 5, such as misstatements regarding the quantity of relevant email correspondence, were designed to save litigation costs and avoid scrutiny by regulators and law enforcement." (*Id.*)

In May 2012, Huawei Device USA asked Company 5 "to sell or license its proprietary robotic system for testing phones," which Company 5 declined to do. (*Id.* ¶ 35.) Subsequently, Huawei and Huawei Device "began to develop their own robotic phone-testing system," and

directed Huawei Device USA employees "to provide detailed information about Company 5's technology to support that effort." (*Id.*)

In August 2012, Huawei Device USA and Company 5 entered into confidentiality agreements that granted Huawei Device USA employees access to Company 5's robotics lab. (*Id.* ¶ 36.) On November 6, 2012, a Huawei engineer emailed a Huawei Device USA employee a "reminder" for "the information we need to build our own robot system," and a file "requesting information about the technical specifications of [Company 5's] robot hardware components and software systems." (*Id.*) The Huawei Device USA employee responded that Huawei Device USA engineers "accessed" Company 5's laboratory and knew how the robots worked and "systems info." (*Id.*) The employee wrote that he "asked them to write down the info in detail and then send to" Huawei and Huawei Device. (*Id.*)

Over the next several months, in violation of the confidentiality agreements, Huawei Device USA employees sent Huawei and Huawei Device "multiple photographs" of Company 5's "secure" laboratory, as well as its robot and software interface system. (*Id.* ¶ 37.) A Huawei Device USA engineer suggested that Huawei and Huawei Device send an engineer to Company 5's laboratory. (*Id.*) Huawei and Huawei Device "continued to develop their own robot while directing [Huawei Device USA] employees to provide more information about Company 5's robot." (*Id.*)

In May 2013, Huawei sent an engineer to Company 5's laboratory "for reconnaissance and [to] obtain measurement data." (*Id.* ¶ 38.) On May 13 and 14, 2013, Huawei Device USA employees used their access badges to let the Huawei engineer into Company 5's laboratory, where the engineer took photographs and "gathered technical information about the robot." (*Id.* ¶ 39.) Company 5 escorted the engineer from the facility, but the engineer sent the photographs

and information to Huawei, Huawei Device, and Huawei Device USA. (*Id.*) Later that month, on May 29, 2013, a Huawei Device USA employee stole a "robot arm" from the laboratory and sent measurements and photographs to Huawei and Huawei Device. (*Id.* ¶ 40.) Huawei Device USA returned the arm after Company 5 discovered the theft. (*Id.*)

In August 2013, Huawei Device USA purported to do an internal investigation of the theft and of the engineer's unauthorized entry into Company 5's laboratory. (*Id.* ¶ 41.) Huawei Device USA issued an "Investigation Report" in which it described its conduct and the engineer's conduct in the laboratory as "isolated incidents," and the theft of the arm as a "moment of indiscretion." (*Id.*) A Huawei Device USA employee claimed falsely that there were "not a lot of emails" discussing Company 5's technology. (*Id.*) In a May 19, 2014 letter to Company 5, Huawei claimed that it had taken "disciplinary measures" in response to the incidents described above. (*Id.* ¶ 42.) Company 5 subsequently sued Huawei, Huawei Device, and Huawei Device USA. (*Id.* ¶ 43.)

i. Company 6

Company 6, a "direct competitor" of Huawei headquartered in California, developed "architecture for memory hardware." (*Id.* ¶¶ 45–46.) Between 2013 and 2018, Huawei schemed to misappropriate Company 6's technology, so that Huawei could "save on research and development costs in the development of its own architecture for memory hardware." (*Id.* ¶¶ 45, 58.)

In 2015, Huawei circulated an internal presentation outlining "countermeasures" it planned to take against Company 6, including "continuously" recruiting Company 6 employees to create "internal turmoil" at Company 6. (*Id.* ¶ 46.) The presentation also included information about employees in the United States and China. (*Id.*)

In June 2015, at Huawei's invitation, Company 6 employees made a presentation in China about its data storage technology. (*Id.* ¶ 47.) Huawei asked for the slides, which Company 6 provided on the condition that Huawei not share them with a competing subsidiary. (*Id.*) Huawei agreed, but then "[i]mmediately" distributed the slides to its engineers, including the competing subsidiary, who discussed how to apply the information to Huawei's designs. (*Id.*)

In 2016, a Huawei engineer visited Company 6's California headquarters under the pretense of discussing an agreement between the companies. (*Id.* ¶ 48.) After a Company 6 "principal" gave a Huawei engineer an "overview" of its design plan, the engineer sent an internal email with a slide deck describing Company 6's intellectual property; the engineer also stated that Huawei's plan for similar technology was "good but we acted a bit late." (*Id.*) Huawei did not pursue a business relationship with Company 6. (*Id.* ¶ 49.)

According to the indictment, Huawei used a "proxy" — a professor — to get information about Company 6's technology. (*Id.* ¶ 50.) Huawei hired the professor in December 2016 to develop "prototype software for memory hardware." (*Id.* ¶ 51.) The professor, without disclosing his relationship to Huawei, asked Company 6 for access to its "prototype board," which contained its "proprietary chip," for "research purposes." (*Id.*)

Two months later, Company 6 and the professor entered into a licensing agreement granting the professor access to the prototype board subject to certain conditions, including prohibitions against disclosing, modifying, or transferring the rights or usage of the technology. (*Id.* ¶¶ 52–53.) Company 6 gave the professor the product number and "the identity of its PRC-based distributor," which were "sensitive proprietary information." (*Id.* ¶ 53.) Company 6 would not have entered into the agreement had it known that the professor was affiliated with

Huawei, "a direct competitor of Company 6." (*Id.* ¶ 52.) After supply chain issues delayed delivery of the board, the professor asked Company 6 to expedite delivery, claiming that he had students to help him with research. (*Id.* ¶ 54.) In fact, the professor wanted the board for a project he had with Huawei; he wrote Huawei that his "dilemma" was that Company 6's "equipment" was not yet available." (*Id.*)

The professor ultimately received the board in April 2017, and gave Huawei the product number, distributor identity, and performance testing results. (*Id.* ¶¶ 55–56.)[4] Huawei used the information in an effort to get a board directly from Company 6's distributor, but the distributor refused; the distributor also told Company 6 that Huawei had tried to get the board. (*Id.* ¶ 55.) The professor denied giving Huawei the product number or the distributor, and Huawei refused to answer Company 6's questions about how it got that information. (*Id.*)

In July 2017, Huawei asked Company 6 for a "high level meeting," purportedly to discuss a business relationship. (*Id.* ¶ 57.) In fact, according to an internal Huawei email, Huawei's real goal was to obtain Company 6's board and "support the development of [Huawei's] two projects" with the professor. (*Id.*) At the meeting, Huawei asked for samples of the board, which Company 6 would not provide without a nondisclosure agreement. (*Id.*) Huawei did not disclose its relationship with the professor, and the partnership between Huawei and Company 6 never materialized. (*Id.*)

b. Defrauding Financial Institutions

The indictment alleges that as "part of its international business model," Huawei "participated in business in countries subject to U.S., E.U. and/or U.N. sanctions," including Iran

[4] According to an internal Huawei document from 2017, Huawei wanted to reverse engineer Company 6's technology, and "external resources" — like the professor — could provide "third-party analysis materials" and "external information" to achieve that goal. (*Id.* ¶ 50.)

and North Korea, by "arranging for shipment of [Huawei] goods and services to end users in sanctioned countries . . . through local affiliates in the sanctioned countries." (*Id.* ¶¶ 68–69.) Huawei misrepresented the scope and nature of its business operations to the United States government and "various victim financial institutions" — including four "multinational banking and financial services compan[ies]" identified in the indictment as "Financial Institutions 1, 2, 3, and 4." (*Id.* ¶¶ 64–67, 71.)

Beginning in 2007, Huawei "repeatedly misrepresented" to the United States government and financial institutions that it conducted business in Iran "in a manner that did not violate applicable U.S. law." (*Id.* ¶ 71.) Huawei operated Skycom Tech Co., Ltd. ("Skycom") as "an unofficial subsidiary to obtain otherwise prohibited U.S.-origin goods, technology and services, including banking services" for its Iran-based business "while concealing the link" between the companies. (*Id.* ¶ 70.) Huawei also helped the Iranian government install surveillance equipment used to "monitor, identify and detain protestors during the anti-government demonstrations of 2009 in Tehran," and, through Skycom, employed at least one American citizen. (*Id.*) This conduct violated the United States Department of the Treasury's Office of Foreign Assets Control's ("OFAC's") Iranian Transactions and Sanctions Regulations ("ITSR"), which prohibits, among other things, exporting any goods, technology, or services from the United States or by a United States citizen to Iran. (*Id.*)

The indictment charges that Huawei used Financial Institution 1's United States subsidiary ("Subsidiary 1") to "process U.S.-dollar clearing transactions involving millions of dollars in furtherance of [its] Iran-based business," although it told Financial Institution 1 that it would not do so. (*Id.* ¶ 72.) Between 2011 and 2013, the Wall Street Journal and Reuters reported that Huawei "assisted the Government of Iran to perform domestic surveillance," that

Skycom "had sold and attempted to sell embargoed U.S.-origin goods to Iran in violation of U.S. law," and that Huawei "owned and operated" Skycom. (*Id.* ¶¶ 73–74.) Huawei responded in published official statements in which it disclaimed helping the Iranian government's surveillance efforts and denied that Skycom sold American goods to Iran. (*Id.*) After the 2012 and 2013 Reuters reports, Huawei told the public and Financial Institutions 1, 2, 3, and 4 that "the allegations regarding [its] ownership and control of Skycom were false" and that Huawei complied with United States sanctions, including the ISTR. (*Id.* ¶ 75.) Financial Institutions 1, 2, 3, and 4 continued their banking relationships with Huawei at least in part based on these false representations. (*Id.*)

In March 2013, Huawei told Financial Institution 4 that the company did not conduct business in North Korea — despite the fact that internal Huawei documents showed that the company was "involved in numerous projects in North Korea beginning no later than 2008." (*Id.* ¶¶ 81–82.)[5]

In August 2013, Wanzhou Meng, Huawei's Chief Financial Officer, met with Financial Institution 1 and gave a presentation which included the following misrepresentations:

> (1) HUAWEI "operates in Iran in strict compliance with applicable laws, regulations and sanctions of UN, US and EU"; (2) "Huawei has never provided and will never provide any technology, product, or service for monitoring communications flow, tracking user locations, or filtering media contents in the Iranian market"; (3) "HUAWEI's engagement with SKYCOM is normal business cooperation"; (4) the defendant WANZHOU MENG's participation on the Board of Directors of SKYCOM was to "help HUAWEI to better understand SKYCOM's financial results and business performance, and to strengthen and monitor SKYCOM's compliance"; and (5) "HUAWEI subsidiaries in sensitive

[5] The indictment alleges that Huawei referred to sanctioned nations such as Iran and North Korea with codenames given the "sensitivity of conducting business in jurisdictions subject to U.S., E.U. and/or U.N. sanctions." (*Id.* ¶¶ 69, 82.)

> countries will not open accounts at [Financial Institution 1], nor have business transactions with [Financial Institution 1]."

(*Id.* ¶¶ 76–77.) On September 3, 2013, at the request of a Financial Institution 1 "executive," Meng "arranged for an English-language version of the . . . presentation to be delivered to Financial Institution 1." (*Id.* ¶ 76.)

In 2014, Meng arrived at John F. Kennedy International Airport in New York, carrying an electronic device with "Suggested Talking Points" about Huawei's relationship with Skycom and Iran, including that Skycom "was established in 1998 and is one of the agents for Huawei products and services" and was "mainly an agent for Huawei." (*Id.* ¶ 78.)[6]

In 2017, after Financial Institution 1 unilaterally ended its relationship with Huawei because of "risk concerns" about Huawei's business practices, Huawei "took steps to secure and expand its banking relationships with other financial institutions," including Financial Institution 4's United States subsidiary ("Subsidiary 4"). (*Id.* ¶¶ 83–84.) In "meetings and correspondence with representatives of" Subsidiary 4, Huawei employees "falsely represented" that the company ended the relationship with Financial Institution 1 based on its "level of service." (*Id.*) Subsidiary 4 then "expand[ed] its banking relationship" with Huawei to permit Huawei to "receive[] income indirectly in the form of cost savings and the value of continued banking services." (*Id.* ¶¶ 85–86.)

The indictment also alleges that Huawei and Huawei Device USA learned of the government's investigation in 2017, and then "made efforts to move witnesses with knowledge about [Huawei's] Iran-based business" to China and "destroy and conceal evidence" of Huawei's Iran-based business. (*Id.* ¶ 87.)

[6] The indictment charges that this file was "in unallocated space—indicating that the file may have been deleted." (*Id.*)

c. False Statements to the United States Government

The indictment alleges that as "part of the efforts . . . to establish and operate its business, particularly in the United States," the defendants made "false statements to the U.S. government" about their scheme to misappropriate the intellectual property of other companies and the "scope of [Huawei's] business activities related to sanctioned countries" like Iran and North Korea. (*Id.* ¶ 59.) Huawei made these false statements to "avoid the economic and regulatory consequences of making truthful statements, including the restriction . . . from U.S. markets and business opportunities." (*Id.*)

In July 2007, the Federal Bureau of Investigation interviewed Huawei's founder, who said that Huawei "did not conduct any activity in violation of" and "operated in compliance with" United States export laws. (*Id.* ¶ 60.) He also said that Huawei "won" Company 1's lawsuit, and that Company 1's chief executive officer would "testify" that Huawei "did not engage in intellectual property rights violations." (*Id.*)

In September 2012, a Huawei "Senior Vice President" testified before the United States House of Representatives' Permanent Select Committee on Intelligence ("HPSCI"), in connection with HPSCI's investigation into national security threats from Chinese telecommunications companies. (*Id.* ¶¶ 61–62.)[7] The indictment charges that the Senior Vice President "falsely testified" that Huawei provided its source code for Company 1 to review, that Company 1 did not find "any infringement," and that this source code was "from a third party partner" and was "available and opened on the Internet." (*Id.* ¶ 62.) The Senior Vice President also testified that Huawei had not violated any sanctions-related laws concerning Iran or

[7] The Senior Vice President is identified in the indictment as "corporate senior vice president under the chief Huawei representative to the United States" who also held the title of "President of Huawei North America." (*Id.* ¶ 62.)

provided any equipment to the Iranian government. (*Id.*) In addition, Huawei submitted a chart that omitted Huawei clients with connections to the Iranian government and "falsely reflect[ed]" that Huawei did not conduct any business in North Korea after 2009. (*Id.* ¶ 63.)

II. Procedural Background

On August 22, 2018, Huawei, Huawei Device, Skycom, and Meng were charged in an eleven-count indictment, which alleged a scheme to defraud financial institutions and skirt United States sanctions in furtherance of Huawei's business in Iran. (ECF No. 25.)[8] The original indictment accused the defendants of conspiracy to defraud the United States, bank fraud and conspiracy to commit bank fraud, wire fraud and conspiracy to commit wire fraud, violations and conspiracy to commit violations of the IEEPA,[9] money laundering conspiracy, and conspiracy to obstruct justice. (*Id.* ¶¶ 25–47.)

The government has since filed three superseding indictments, on December 6, 2018 (ECF No. 24), January 24, 2019 (ECF No. 19), and February 13, 2020 (ECF No. 126). The first superseding indictment added two charges: a bank fraud conspiracy count and substantive bank fraud count. (ECF No. 24 ¶¶ 25–26, 31–32 (Counts 2 and 5).)[10] The second superseding indictment added factual allegations. (ECF No. 19.) The third superseding indictment added Huawei Device and Futurewei as defendants (ECF No. 126), as well as the following additional charges: racketeering conspiracy, conspiracy to steal trade secrets, and conspiracy to commit wire fraud in connection with the defendants' misappropriation of intellectual property (*id.* ¶¶ 88–98 (Counts 1–3)).

---

[8] The original indictment also named a fourth company, under seal, as a defendant. (ECF No. 25.) The government dropped this defendant from the case in the first superseding indictment. (ECF No. 24.)

[9] The original indictment contained two substantive IEEPA violation charges and two conspiracy to violate IEEPA charges. (ECF No. 25 ¶¶ 36–43 (Counts 6–9).)

[10] The first superseding indictment also added two individual defendants, under seal. (ECF No. 24.)

On November 8, 2024, the defendants moved to dismiss Counts 1 through 12 and Count 15 of the indictment. The Court heard oral argument on May 14, 2025.

LEGAL STANDARD

Federal Rule of Criminal Procedure 7 requires that an indictment contain a "plain, concise, and definite written statement of the essential facts constituting the offense charged." Fed. R. Crim. P. 7(c)(1). An indictment satisfies this rule if it "first, contains the elements of the offense charged and fairly informs a defendant of the charge against which he must defend, and, second, enables him to plead an acquittal or conviction in bar of future prosecutions for the same offense." *United States v. Stringer*, 730 F.3d 120, 124 (2d Cir. 2013) (quoting *Hamling v. United States*, 418 U.S. 87, 117 (1974) (internal quotation marks omitted)).

Thus, an indictment "need do little more than to track the language of the statute charged and state the time and place (in approximate terms) of the alleged crime." *United States v. Yannotti*, 541 F.3d 112, 127 (2d Cir. 2008) (citation omitted); *see also Hamling,* 418 U.S. at 117 ("It is generally sufficient that an indictment set forth the offense in the words of the statute itself, as long as 'those words of themselves fully, directly, and expressly, without any uncertainty or ambiguity, set forth all the elements necessary to constitute the offence intended to be punished.'" (citation omitted)). Indictments do not "have to specify evidence or details of how the offense was committed." *United States v. Wey*, No. 15-CR-611, 2017 WL 237651, at *5 (S.D.N.Y. Jan. 18, 2017) (citations omitted). Moreover, a court considering "[a] pretrial motion to dismiss an indictment must not weigh the sufficiency of the evidence." *United States v. Tucker*, No. 16-CR-91, 2017 WL 3610587, at *2 (S.D.N.Y. Mar. 1, 2017) (citing *United States v. Alfonso*, 143 F.3d 772, 777 (2d Cir. 1998)). Finally, "[w]hen considering a motion to dismiss, the Court must treat the indictment's allegations as true." *Wey*, 2017 WL 237651, at *5 (citing

United States v. Velastegui, 199 F.3d 590, 592 n.2 (2d Cir. 1999), *cert. denied*, 531 U.S. 823 (2000)); *Coffey*, 361 F. Supp. 2d at 111.

A defendant seeking dismissal of an indictment "faces a high standard." *United States v. Xu*, No. 23-CR-133-5, 2024 WL 1332548, at *1 (S.D.N.Y. Mar. 28, 2024) (quoting *United States v. Chastain*, No. 22-CR-305, 2022 WL 13833637, at *2 (S.D.N.Y. Oct. 21, 2022)); *see also United States v. Broward*, 594 F.2d 345, 351 (2d Cir. 1979). "Dismissal of charges is an extraordinary remedy reserved only for extremely limited circumstances implicating fundamental rights." *United States v. Bankman-Fried*, 680 F. Supp. 3d 289, 304 (S.D.N.Y. 2023) (citation and internal quotations omitted); *see also United States v. De La Pava*, 268 F.3d 157, 165 (2d Cir. 2001).

Accordingly, the court's review on a motion to dismiss the indictment is limited to "determining whether the grand jury has performed its function under the Sixth Amendment . . . by finding all of the essential elements of the crime." *United States v. Phillips*, 690 F. Supp. 3d 268, 277 (S.D.N.Y. 2023). "[A] federal indictment can be challenged on the ground that it fails to allege a crime within the terms of the applicable statute" because "the grand jury will not have found one or more of the elements necessary to bind a defendant over for trial." *Id.* at 277–78 (quoting *United States v. Aleynikov*, 676 F.3d 71, 75–76 (2d Cir. 2012)). The Court must also "determin[e] whether the defendant has been sufficiently informed of the crime of which he is accused so as to plead double jeopardy as a bar to a subsequent prosecution." *Id.* at 278 (citations omitted). In conducting this inquiry, the Court "will not look beyond the face of the indictment and draw inferences as to the proof to be adduced at trial, for the sufficiency of the evidence is not appropriately addressed on a pretrial motion to dismiss." *Bankman-Fried*, 680 F. Supp. 3d at 304 (cleaned up).

DISCUSSION

I. Count 1: Racketeering Conspiracy

The defendants cite three bases for dismissing Count 1. First, they claim that the intra-corporate conspiracy doctrine bars prosecution for racketeering. (ECF No. 474-1 at 10–11.) Second, they maintain that the indictment does not sufficiently allege that they conspired to use racketeering-derived funds. (*Id.*) Finally, they say that the indictment does not allege a pattern of racketeering activity. (*Id.*)[11] As explained below, these arguments are not persuasive.

Count 1 of the indictment charges the defendants and Skycom with racketeering conspiracy. (ECF No. 126 ¶¶ 88–93.) Section 1962(a) makes it illegal "for any person who has received any income derived, directly or indirectly, from a pattern of racketeering activity" and who "participated as a principal" to "use or invest, directly or indirectly, any part of such income, or the proceeds of such income, in . . . the establishment or operation of, any enterprise" affecting interstate commerce. 18 U.S.C. § 1962(a). Section 1962(d) makes it "unlawful for any person to conspire" to violate Section 1962(a). *Id.* § 1962(d).

The government alleges that the defendants and Skycom constituted an "enterprise" whose purpose was to "grow the global 'Huawei' brand into one of the most powerful telecommunications . . . companies in the world by entering, developing and dominating the

[11] The defendants also argue that "Count One should be dismissed for several reasons related to the alleged RICO 'enterprise.'" (*Id.* at 28.) The defendants concede, however, that two of these reasons — that the "distinctness" requirement set forth in Section 1962(c) applies to Section 1962(a) and that an association-in-fact enterprise does not encompass an enterprise consisting solely of corporations — are foreclosed by Second Circuit precedent. (*Id.* at 28–29 (citing *Riverwoods Chappaqua Corp. v. Marine Midland Bank, N.A.*, 30 F.3d 339, 345 (2d Cir. 1994); *United States v. Huber*, 603 F.2d 387, 393–94 (2d Cir. 1979)).) Additionally, the defendants argue, without citing any case law, that Count 1 must be dismissed because it "fails to allege that the income from a pattern of racketeering activity was invested in an enterprise *other than* the entity that generated the income." (*Id.* at 29.) Section 1962(a) does not require that income derived from a racketeering enterprise be invested in a different enterprise. *See* 18 U.S.C. § 1962(a); (ECF No. 496 at 28–29.) And, in any event, the extent to which the income was invested in the racketeering enterprise or another entity depends on the evidence at trial.

markets for telecommunications and consumer electronics technology and services" in the countries where the enterprise operated. (ECF No. 126 ¶ 90.) The indictment states that from 1999 to the present, Huawei, Huawei Device, and Huawei Device USA were "principals" of the enterprise and "knowingly and intentionally conspire[d]" to "use and invest" income derived from a pattern of racketeering activity "in the establishment and operation" of the enterprise, "the activities of which affected, interstate and foreign commerce." (*Id.* ¶ 92.) The indictment alleges that the "pattern of racketeering activity" included wire fraud, bank fraud, obstruction of justice, witness tampering, theft of trade secrets, money laundering, and copyright infringement. (*Id.* ¶ 93.)

a. Intra-Corporate Conspiracy Doctrine

First, the defendants cite the "intra-corporate conspiracy doctrine" for the proposition that a "parent company cannot form a conspiracy with its wholly owned subsidiary, or those subsidiaries with one another." (ECF No. 474-1 at 15.) Under this doctrine — which the Supreme Court established in *Copperweld Corp. v. Indep. Tube Corp.*, 467 U.S. 752, 771 (1984) — "business units of a company have to communicate and agree with one another" and that "in view of the increasing complexity of corporate operations, a business enterprise should be free to structure itself in ways that serve efficiency of control . . . without increasing its exposure to antitrust liability." (ECF No. 474-1 at 16 (quoting *Copperweld*, 467 U.S. at 773).) *Copperweld,* however, was not a criminal case; it was an antitrust case, and the Supreme Court framed the intra-corporate conspiracy doctrine in that context. Nevertheless, the defendants argue that the *Copperweld* "rationale . . . applies with full force to the conspiracy to violate 18 U.S.C. § 1962(a)." (*Id.* at 16.)

The government responds that the *Copperweld* "considerations do not apply in the context of criminal conspiracies" because "combined criminal activity—even within a corporate enterprise—is more 'dangerous to the public' than crimes committed alone." (ECF No. 496 at 16–17 (quoting *Salinas v. United States*, 522 U.S. 52, 65 (1997)). The government also points out that "[e]very Circuit to have considered the question has thus held that the intracorporate conspiracy doctrine is inapplicable to criminal prosecutions." (*Id.* at 17–18 (collecting cases).)

The simple answer to the defendants' claim is that there is no precedent for it. No court — in this circuit or elsewhere — has applied the intra-corporate conspiracy doctrine to a criminal case, RICO or otherwise. On the contrary, every court to have considered the question has concluded that the intra-corporate conspiracy doctrine does not apply to criminal conspiracies. *United States v. St. John*, 625 F. App'x 661, 665 (5th Cir. 2015); *United States v. Basroon*, 38 F. App'x 772, 781 (3d Cir. 2002); *McAndrew v. Lockheed Martin Corp.*, 206 F.3d 1031, 1035 (11th Cir. 2000); *United States v. Hughes Aircraft Co.*, 20 F.3d 974, 979 (9th Cir. 1994), *as amended* (Apr. 28, 1994); *United States v. Ames Sintering Co.*, 927 F.2d 232, 237 (6th Cir. 1990); *United States v. Hugh Chalmers Chevrolet-Toyota, Inc.*, 800 F.2d 737, 738 (8th Cir. 1986); *United States v. Peters*, 732 F.2d 1004, 1008 (1st Cir. 1984). This Court sees no reason to depart from the sound logic behind those decisions.

As the Supreme Court explained in *Cedric Kushner Promotions, Ltd. v. King*, 533 U.S. 158, 166 (2001), the "intracorporate conspiracy doctrine . . . turns on specific antitrust objectives." The doctrine "was a product of" the "corporate entity fiction [that] was designed to expand corporate liability by holding the corporation liable for the acts of its agents." *McAndrew*, 206 F.3d at 1040. Because "criminal conspiracies pose the precise group danger at which conspiracy liability is aimed . . . the corporate entity doctrine in such cases [is] a 'fiction

without a purpose.'" *Id.* (quoting *Dussouy v. Gulf Coast Inv. Corp.*, 660 F.2d 594, 603 (5th Cir. 1981)); *see also United States v. Wise*, 370 U.S. 405, 417 (1962) (Harlan, J. concurring) ("[T]he fiction of corporate entity, operative to protect officers from contract liability, had never been applied as a shield against criminal prosecutions. . . .").[12]

[redacted]

To the extent that this is an argument about the sufficiency of the evidence, that is not cognizable on a motion to dismiss an indictment. Under Rule 12(b), a defendant may "raise by pretrial motion any defense, objection, or request that the court can determine without a trial on the merits," but "a defense [that] raises dispositive 'evidentiary questions,' [requires] a district court [to] defer resolving those questions until trial." *United States v. Sampson*, 898 F.3d 270,

[12] Both parties acknowledge that there is a circuit split about whether the intra-corporate conspiracy doctrine applies in civil RICO cases, and that the Second Circuit has not yet addressed the issue. (ECF No. 496 at 18; ECF No. 515 at 11–12.) However, Judge Lewis Liman and Judge Jesse Furman, in meticulous and well-reasoned opinions, concluded that the intra-corporate conspiracy doctrine does not apply in that context. *Lateral Recovery LLC v. Funderznet LLC*, No. 22-CV-2170, 2024 WL 4350369, at *40 (S.D.N.Y. Sept. 27, 2024); *Alix v. McKinsey & Co., Inc.*, No. 18-CV-4141, 2023 WL 5344892, at *23 (S.D.N.Y. Aug. 18, 2023).

279 (2d Cir. 2018) (citations omitted). The exception to this rule is when "the government has made what can fairly be described as a full proffer of the evidence it intends to present at trial." *Alfonso*, 143 F.3d at 776; *see also United States v. Wedd*, 993 F.3d 104, 121 (2d Cir. 2021) ("The district court must give the Government an opportunity to make a detailed presentation of the entirety of the evidence before dismissing an indictment on sufficiency grounds, and the district court lacks the authority to require the government, before trial, to make such a presentation as this could effectively force a summary judgment-like motion on the government." (cleaned up)).

Determining [redacted] "requires the Court to analyze the sufficiency of the Government's evidence, which the Court is not permitted to do on a motion to dismiss." *Phillips*, 690 F. Supp. at 288; *see also United States v. Perez*, 575 F.3d 164, 166–67 (2d Cir. 2009) ("[T]he sufficiency of the evidence is not appropriately addressed on a pretrial motion to dismiss an indictment."); *United States v. Kelly*, 462 F. Supp. 3d 191, 197 (E.D.N.Y. 2020) ("The Government is entitled to marshal and present its evidence at trial, and the defendant is entitled to challenge the sufficiency of that evidence pursuant to Rule 29 of the Federal Rules of Criminal Procedure."). The government has not "offer[ed] a full proffer of its trial evidence at this time." (ECF No. 496 at 21.)

b. Use of Racketeering Income

Second, the defendants argue that Count 1 must be dismissed because the indictment does not "allege any *domestic* use or investment of the funds at issue." (ECF No. 474-1 at 19.) According to the defendants, a Section 1962(a) racketeering charge "is presumed to be limited to domestic use or investment of proceeds derived from a pattern of racketeering." (*Id.* at 21.) The defendants maintain that "the only plausible way to read the Indictment is that the relevant investment of racketeering income was in *Chinese* businesses," not domestic businesses; thus,

the defendants say, Count 1 is legally deficient on its face and must be dismissed. (ECF No. 515 at 14.)

The government responds that the defendants are arguing extraterritoriality, which is "premature, as it turns on the defendants' speculation about the evidence to be introduced at trial." (ECF No. 496 at 22.) Moreover, the government asserts, "the Huawei Enterprise includes all U.S. affiliates and subsidiaries of Huawei Tech." (*Id.* at 25.) While emphasizing that it "has not provided, and does not here provide, a full proffer of its trial evidence," the government "expects to demonstrate at trial that there is 'conduct relevant to the statute's focus occur[ing] in the United States.'" (*Id.* (quoting *RJR Nabisco, Inc. v. European Cmty.*, 579 U.S. 325, 337 (2016)).) The government further disputes the defendants' claim that "the only plausible way to read the Indictment" is that the defendants invested the income they derived from the racketeering activity only in Huawei's Chinese businesses. (ECF No. 515 at 14.)

The government has the better argument. The defendants are asking the Court to evaluate the sufficiency of the evidence, which the Court cannot do on a motion dismiss the indictment. In any event, the indictment alleges that Huawei Device USA — an American subsidiary — was part of the racketeering enterprise and that the defendants conspired to "use and invest, directly and indirectly, a part of income . . . in the establishment and operation of the Huawei Enterprise." (ECF No. 126 ¶¶ 3, 92.) That is sufficient at this stage of the proceedings. The trial evidence will demonstrate whether the defendants engaged in a pattern of racketeering activity and whether the defendants invested the income from that activity in businesses with sufficient domestic ties. The government is entitled to "an opportunity to make a detailed presentation of the entirety of [that] evidence." *Wedd*, 993 F.3d at 121.

c. Pattern of Racketeering Activity

Third, the defendants assert that the government has not alleged a "pattern of racketeering" because "the predicate acts on which the government relies are *not* adequately related." (ECF No. 474-1 at 25.) Pointing out that the government "must prove at least two predicate racketeering acts that 'amount to or pose a threat of continued criminal activity' and are 'related'" (*id.* at 24 (citations omitted)), the defendants argue that Count 1 "fuses together categorically different alleged crimes—one group relating to the trade secret charges . . . and another relating to the fraud and sanctions charges" that have "no connective tissue" (*id.* at 26). The defendants say that the "trade secret charges . . . involve different companies, different technologies, different Huawei personnel, different methods, different locations, and different timeframes over the space of twenty years," which "are not otherwise interrelated." (*Id.*) As for the sanctions-related charges, the defendants contend that "the alleged acts of wire fraud, bank fraud, and sanctions violations all involved different transactions with different banks involving different Huawei personnel." (*Id*. at 27.)[13]

This argument, too, is a sufficiency of the evidence argument. "While there is no Second Circuit ruling directly on point, other case law indicates overwhelmingly that the Government does *not* have to plead either subpart of the 'pattern' element—relatedness or continuity." *United States v. Raniere*, 384 F. Supp. 3d 282, 301 (E.D.N.Y. 2019); *accord United States v. Cooper*, No. 17-CR-296, 2020 WL 2307646, at *4 (E.D.N.Y. May 8, 2020). Rather, "at most, an indictment need only specify predicate acts "that evidence continuity and relatedness." *Raniere*,

[13] The defendants also assert that fraud charges "are no longer viable in light of *Ciminelli v. United States*, 598 U.S. 306 (2023)" and that the sanctions charges "cannot serve as predicates under § 1962(a) because they do not allege any cognizable 'income' that could be invested into the alleged RICO enterprise." (*Id.*) The Court addresses the *Ciminelli* claim in Section III of this opinion.

384 F. Supp. 3d at 301 (citing *United States v. Giovannelli*, No. 01-CR-749, 2004 WL 48869, at *3 (S.D.N.Y. Jan. 9, 2004)); *see also United States v. Messina*, No. 11-CR-31, 2012 WL 463973, at *4 (E.D.N.Y. Feb. 13, 2012) ("[The] defendant's arguments that the Indictment 'fails to show any meaningful relationship between the four racketeering acts' and 'attempt[s] to rope together a series of separate mini-conspiracies committed by isolated actors' are premature, as they confuse the standards of pleading with standards of proof."); *United States v. Basciano*, No. 03-CR-929, 2006 WL 8451578, at *20 (E.D.N.Y. Jan. 3, 2006) ("[D]etermining the 'relatedness' of racketeering acts in a RICO case is inappropriate at the pre-trial stage."); *United States v. Torres*, 191 F.3d 799, 806–07 (7th Cir. 1999) ("[A]n indictment does not have to allege continuity, which is not an element of the offense, with particularity.").

II. Counts 2 and 3: Trade Secrets Charges

Counts 2 and 3 of the indictment charge the defendants with conspiring to steal trade secrets[14] and to commit wire fraud.[15] (ECF No. 126 ¶¶ 94–98.) Count 2 charges that the defendants "knowingly, and with intent to convert one or more trade secrets that were related to a product used in or intended for use in interstate and foreign commerce, conspired to . . . steal . . . copy . . . and receive, buy and possess such trade secrets" for their economic benefit. (*Id.* ¶ 95.)[16] In addition, Count 2 charges that the defendants "intend[ed] or [knew] that the offense

[14] 18 U.S.C. § 1832 makes it unlawful to steal, duplicate, or receive "a trade secret that is related to a product" used in interstate commerce with the intent to convert that trade secret and knowledge that doing so will "injure any owner of that trade secret." 18 U.S.C. § 1832(a)(1) – (3). Section 1832(a)(5) makes it illegal to conspire to violate Section 1832(a)(1) – (3).

[15] A defendant commits wire fraud in violation of 18 U.S.C. § 1343 when, "having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, [it] transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice." 18 U.S.C. § 1349 prohibits conspiring to commit wire fraud.

[16] A "trade secret" encompasses all "scientific, technical, economic, or engineering information . . . [that] the owner thereof has taken reasonable measures to keep . . . secret; and [which] derives independent

would injure any owner of those trade secrets." (*Id.*) The indictment lists eleven "overt acts" in furtherance of the conspiracy:

(1) In March 2002, a Futurewei employee "contacted an employee of Company 1 . . . regarding potential employment" with Futurewei, "in an attempt to misappropriate trade secret information" belonging to Company."

(2) On March 3, 2003, "at the request of" a Huawei engineer, a Company 2 employee "wrote an email to" Huawei employees" "which comprised and included trade secret information, bearing the markings 'HIGHLY CONFIDENTIAL' and '[Company 2] Confidential Property;'"

(3) On July 11, 2007, a Huawei employee told FBI agents that Huawei "won" its lawsuit with Company 1 and that Company 1's CEO would "testify" that Huawei "did not engage in intellectual property rights violations."

(4) On October 30, 2009, Futurewei "filed a provisional patent application with the U.S. Patent and Trademark Office that used and relied upon in large part misappropriated Company 4 trade secret information."

(5) On September 13, 2012, a Huawei Senior Vice President "falsely testified before U.S. Congress that 'As specifically to the source code [allegedly stolen from Company 1], the source code of the issues was actually from a third party partner . . . already available and open on the internet.'"

(6) On May 29, 2013, a Huawei Device USA employee "accessed a Company 5 laboratory and surreptitiously placed a robot arm, which comprised and included trade secret information of Company 5, into a laptop bag" and removed it from the laboratory.

(7) In July 2013, Huawei and Huawei Device "launched a formal policy to encourage employees to steal confidential information from competitors."

(8) On June 9, 2015, after Company 6 emailed Huawei "a presentation marked 'Proprietary and Confidential'" that described "Company 6's architecture for solid state drives," Huawei "distributed [the presentation] internally, notwithstanding oral promises to maintain confidentiality and not to distribute the information."

(9) On June 18 and 21, 2017, Huawei "tried unsuccessfully to purchase Company 6's nonpublic proprietary technology directly from the Distributor without Company 6's permission and without informing Company 6."

---

economic value . . . from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information." 18 U.S.C. § 1839(3).

(10) On August 2, 2017, a professor "emailed testing results of software run on" Company 6's technology to Huawei, "contrary to the Agreement between the Professor and Company 6, which expressly prohibited the direct or indirect transfer of rights or usage in the [technology] to third parties."

(11) In 2017, Huawei "circulated an internal memorandum calling for the use of reverse engineering teams which would rely on external resources to obtain third-party analysis of nonpublic intellectual property belonging to other companies."

(*Id.* ¶ 96.)

Count 3 — wire fraud conspiracy — alleges that the defendants "knowingly and intentionally conspire[d] to devise a scheme and artifice to defraud" Companies 1 through 6 and "to obtain money and property from" those companies "by means of one or more materially false and fraudulent pretenses, representations and promises" and "for the purpose of executing such scheme and artifice" to "transmit and cause to be transmitted by means of wire communication in interstate and foreign commerce, writings, signs, signals, pictures and sounds." (*Id.* ¶ 98.)

The defendants maintain that Counts 2 and 3 are impermissibly duplicitous and violate due process. Neither argument is persuasive.

a. Duplicity

The defendants contend that Counts 2 and 3 are "impermissibly duplicitous" because they "encompass multiple alleged conspiracies." (ECF No. 474-2 at 12.) While they concede that "the question of whether conduct constitutes a single conspiracy is typically reserved for the jury," they claim that the Court has the authority to dismiss these counts because the charges are "obviously duplicitous from the face of the indictment." (*Id*.) The defendants emphasize that "each of the six" trade secret allegations "involves [different c]ompanies, different alleged trade secrets, different individuals, different methods, and different . . . timeframes over a span of twenty years." (*Id.* at 14.) Because "the Indictment contains 'no set of facts' from which a jury

could find the single conspiracy alleged," the defendants argue that the government's "boilerplate allegation" of a single conspiracy is insufficient. (ECF No. 515 at 18.)

The government responds that a jury should decide the scope of the conspiracies charged in Counts 2 and 3 — including whether the indictment alleges single conspiracies or multiple conspiracies. (ECF No. 496 at 31–33.) In any event, the government argues, "a count is not duplicitous merely because it alleges a single agreement 'to commit several crimes' . . . because the conspiracy is accomplished 'by several means,'" or because "it could have been charged as multiple conspiracies." (*Id.* at 34 (quoting *United States v. Murray*, 618 F.2d 892, 896 (2d Cir. 1980)).) Rather, the government maintains, "the *agreements* at issue in Counts Two and Three extended for the full lengths of the charged period." (*Id.* at 35.)

An indictment is duplicitous if "it joins two or more distinct crimes in a single count." *United States v. Aracri*, 968 F.2d 1512, 1518 (2d Cir. 1992) (citing *Murray*, 618 F.2d at 896). "Duplicitous pleading is not presumptively invalid; rather, it is impermissible only if it prejudices the defendant." *United States v. Ohle*, 678 F. Supp. 2d 215, 221 (S.D.N.Y. 2010) (citing *United States v. Olmeda*, 461 F.3d 271, 281 (2d Cir. 2006)). Conspiracy charges present "unique issues in the duplicity analysis," because acts "that could be charged as separate counts of an indictment may instead be charged in a single count if those acts could be characterized as part of a single continuing scheme." *United States v. Peters*, 543 F. App'x 5, 7–8 (2d Cir. 2013) (quoting *Aracri*, 968 F.2d at 1518). Accordingly, when an indictment "on its face sufficiently alleges a single conspiracy, the question of whether a single conspiracy or multiple conspiracies exists is a question of fact for the jury." *United States v. Rajaratnam*, 736 F. Supp. 2d 683, 688 (S.D.N.Y. 2010) (quoting *Ohle*, 678 F. Supp. 2d at 222); *see also Aracri*, 968 F.2d at 1519 ("Whether the government has proved a single conspiracy or has instead proved 'multiple other

independent conspiracies is a question of fact for a properly instructed jury.'" (quoting *United States v. Alessi*, 638 F.2d 466, 472 (2d Cir. 1980))).

In *United States v. Gabriel*, 920 F.Supp. 498 (S.D.N.Y. 1996), the indictment alleged a six-year conspiracy "to defraud [a company's] customers," but listed "eight overt acts . . . [that] readily divide into four earlier acts taken . . . to further the initial scheme to defraud and four later acts taken . . . to try to cover up the now-discontinued scheme." *Id.* at 503–04 (citation omitted). Although the indictment "appear[ed] to actually allege two distinct conspiracies," the court found that "the determination of whether a conspiracy is single or multiple is an issue of fact 'singularly' well suited to determination by a jury." *Id.* at 504 (citations omitted). The court noted the "boilerplate allegations of a single conspiracy," but could not "conclude on the basis of the pleadings alone that there is *no* set of facts . . . that could warrant a reasonable jury in finding a single conspiracy." *Id.* at 505.

The indictment in *United States v. Ohle*, 678 F. Supp. 2d at 222–23, also made "boilerplate allegations of a single conspiracy," and "subsequent description of the overt acts indicate[d] that [the charge] may consist of multiple conspiracies." Citing *Gabriel*, the court found that the government's allegations "survive[d] the facial test," and that the allegations of temporal proximity, common participants, and shared compensation amongst the co-conspirators were sufficient to "allege[] a single conspiracy on its face." *Id.* at 223.

The allegations in Counts 2 and 3 adequately allege a single conspiracy to steal trade secrets and a single conspiracy to commit wire fraud, even though, as the defendants claim, each conspiracy involve "different [companies], different alleged trade secrets, different individuals, different methods," and conduct that happened over a "span of twenty years." (ECF No. 474-2 at 14.) The indictment tracks the language of 18 U.S.C. §§ 1342, 1349, and 1832, and like the

indictment in *Ohle*, alleges that the defendants benefitted economically from each conspiracy. (ECF No. 126 ¶¶ 95, 98.) Moreover, Count 2 lists overt acts that allege coordination among the defendants and their employees in furtherance of the conspiracy to steal trade secrets. (*Id.* ¶¶ 95–96, 98.) At trial, the government will have to prove a single conspiracy for each count, but the Court cannot conclude at this stage "that there is *no* set of facts . . . that could warrant a reasonable jury in finding a single conspiracy." *Gabriel*, 920 F.Supp. at 505.

The defendants also claim they will have "to defend themselves at trial against alleged theft events for which the statute of limitations has long since expired" and for which "documentary and testimonial evidence . . . has long since been lost." (ECF No. 474-2 at 17–18.) Citing *Gabriel*, the defendants say that they should not have to "defend against stale and ancient charges." (*Id.* at 17 (quoting *Gabriel*, 920 F.Supp. at 507).)

Gabriel does not compel a different result. As explained above, the court rejected the defendant's duplicity argument on the contested conspiracy count but dismissed the charge on statute of limitations grounds. *Gabriel*, 920 F.Supp. at 504–07. The court found that the government tried to "save" the conspiracy count "by filing a first superseding indictment . . . that enlarged the allegations to include the [the defendant's] cover-up activities," which took place several years later. *Id*. at 505; *see also Grunewald v. United States*, 353 U.S. 391, 403 (1957) ("'[A]ttempts to cover up after the crime begins to come to light' cannot alone serve to extend the period of the conspiracy."). Nothing in the indictment in this case suggests "an impermissible attempt to save an otherwise time-barred conspiracy through allegations of acts of concealment that . . . [would] extend the scope and duration of the conspiracy." *Gabriel*, 920 F.Supp. at 505.[17]

[17] The defendants also claim potential "double jeopardy concerns should the government attempt to prosecute one or more Defendant for conduct encompassed by the single conspiracy" charges. (ECF

b. Due Process

The defendants also move to dismiss Counts 2 and 3 on due process grounds. They assert that too much time that has passed with respect to conduct related to Companies 1, 2, and 3, and that the government has not justified the delay. (ECF No. 474-2 at 19.)

The "Due Process Clause has a limited role to play in protecting against oppressive delay." *United States v. Lovasco*, 431 U.S. 783, 789 (1977). To prevail on a due process claim based on pre-indictment delay, a defendant "bears the 'heavy burden' of proving both that he suffered actual prejudice because of the alleged pre-indictment delay *and* that such delay was a course intentionally pursued by the government for an improper purpose." *United States v. Cornielle*, 171 F.3d 748, 752 (2d Cir. 1999) (quoting *United States v. Scarpa*, 913 F.2d 993, 1014 (2d Cir. 1990)); *see also United States v. Ray*, 578 F.3d 184, 199 (2d Cir. 2009) ("[A] defendant must show both prejudice and an unjustified reason for the delay in order to prove a due process violation."). "There is a strong presumption that an indictment filed within the statute of limitations is valid." *United States v. Maxwell*, 534 F. Supp. 3d 299, 316 (S.D.N.Y. 2021), *aff'd*, 118 F.4th 256 (2d Cir. 2024); *see also DeMichele v. Greenburgh Cent. Sch. Dist. No. 7*, 167 F.3d 784, 790–91 (2d Cir. 1999) ("[W]hile the [Supreme] Court may not have shut the door firmly on a contention that at some point the Due Process Clause forecloses prosecution of a claim because it is too old, at most the door is barely ajar.").

A defendant must "make a specific, particularized showing of substantial prejudice to overcome this presumption." *United States v. Jordan*, 629 F. Supp. 3d 49, 54 (E.D.N.Y. 2022)

No. 474-2 at 18.) They say that this concern is "not merely hypothetical" because Huawei and Huawei Device USA are being prosecuted in the Western District of Washington for a "separate trade secret conspiracy" that implicates the conduct related to Company 5. (*Id.* at 18.) Whatever the merits of this claim, it is clearly premature at this stage, when no jury has even been selected, let alone reached a verdict.

(quoting *Cornielle*, 171 F.3d at 752). The "possibility of faded memories, unavailable witnesses, and loss of evidence, by itself, is insufficient." *Id.* (citing *United States v. Marion*, 404 U.S. 307, 324 (1971)); *DeMichele*, 167 F.3d at 791 ("[T]he dimming of memories as a result of delay does not constitute actual prejudice." (citing *United States v. Elsbery*, 602 F.2d 1054, 1059 (2d Cir. 1979)). Rather, the defendants must show "that the delay seriously damaged [its] ability defend against the charges." *Maxwell*, 534 F. Supp. 3d at 316 (citing *Cornielle*, 171 F.3d at 751); *see also United States v. Alharbi*, No. 22-2092, 2024 WL 939629, at *1 (2d Cir. Mar. 5, 2024) ("'Actual prejudice' means prejudice that is not speculative." (quoting *United States v. Birney*, 686 F.2d 102, 105–06 (2d Cir. 1982))). "[P]rosecutors do not deviate from 'fundamental conceptions of justice' when they defer seeking indictments until they have probable cause to believe an accused is guilty." *Lovasco*, 431 U.S. at 790–91.

The decision "to prosecute a defendant following investigative delay does not deprive him of due process, even if his defense might have been somewhat prejudiced by the lapse of time." *United States v. Dinero Express, Inc.*, 57 F. App'x 456, 459 (2d Cir. 2002) (quoting *Lovasco*, 431 U.S. at 796). This is because "compelling a prosecutor to file public charges as soon as the requisite proof has been developed" would "impair the prosecutor's ability to continue his investigation," "pressure prosecutors into resolving doubtful cases in favor of early and possibly unwarranted prosecutions," and "preclude the Government from giving full consideration to the desirability of not prosecuting in particular cases." *Lovasco*, 431 U.S. at 792–94. Thus, a defendant can establish a due process violation only if he proves that the delay was "intentionally pursued by the government for an improper purpose." *Cornielle*, 171 F.3d at 752; *see also United States v. Delacruz*, 970 F. Supp. 2d 199, 203 (S.D.N.Y. 2013) (denying motion to dismiss charges on due process grounds where the defendant had "not made any

showing that the preindictment delay was an intentional device designed by the Government to gain a tactical advantage").

None of the defendants' arguments meet this exacting standard. For example, they claim that they cannot "challenge whether the code actually constituted a trade secret," because the "original source code from the time of the incident" is no longer available, and two potential witnesses are no longer available. (ECF No. 474-2 at 21.) But factual impossibility — in this case, whether Company 1's source code was really a trade secret — is not a defense to a conspiracy charge, which focuses on a defendant's intent. *United States v. Zheng*, 113 F.4th 280, 298 (2d Cir. 2024) ("[T]he government was not required to prove, for purposes of the conspiracy count, that the stolen materials were actually trade secrets."). Nor have the defendants explained what the unavailable witnesses — the neutral expert who opined that Huawei's source code was a copy and a former Company 1 employee who said that Huawei attempted to recruit him in Company 1's civil case against Huawei (ECF No. 126 ¶ 23; ECF No. 474-2 at 21–22) — would say, let alone how their testimony would be helpful to the defendants. *United States v. Scala*, 388 F. Supp. 2d 396, 400 (S.D.N.Y. 2005) (finding the defendant did not establish actual prejudice where there was "no evidence . . . as to what [the unavailable witnesses] would have testified, much less specific evidence of how losing that testimony has caused [the defendant] actual prejudice").

The defendants' claims of prejudice relating to Companies 2 and 3 are similarly speculative. They assert that for Company 2, the government's delay "necessarily hinders" their "ability to rebut the government's allegations without access to the full scope of documentary evidence and the fresh recollection of witnesses that would have been available." (*Id.* at 22.) As for Company 3, they contend that evidence is "no longer available" because, aside from two

documents,[18] they have "received nothing in discovery from the government related to this alleged incident." (*Id.*) Even if that is accurate, however, "faded memories, unavailable witnesses, and loss of evidence, by itself, is insufficient." *United States v. Jordan*, 629 F. Supp. 3d at 54 (citing *Marion*, 404 U.S. at 324); *Maxwell*, 534 F. Supp. 3d at 317 ("[M]issing witnesses, failing memories, or lost records . . . are difficulties that arise in any case where there is extended delay in bringing a prosecution, and they do not justify dismissing an indictment."); *DeMichele*, 167 F.3d at 791.

The defendants also challenge the government's motives. They say that "the government's delay cannot be attributed to any justifiable investigatory purpose" and that "it can be inferred" either that the government was trying to "gain a tactical advantage" or was reckless. (ECF No. 474-2 at 23–24.)[19] The government responds that the indictment is the "the product of a massive international investigation," as part of which it "interviewed scores of witnesses around the world, collected millions of documents, and secured evidence located overseas." (ECF No. 496 at 46.) In addition, the government says, the added complexity of prosecuting corporate defendants and "high-level review within the Department of Justice" made the investigation longer. (*Id.* at 47.)

There is no merit to the defendants' accusation that the government purposefully delayed the case to gain a tactical advantage. This case is unquestionably complex, as the defense counsel has observed at various points in the more than seven years that the case has been

[18] The government, on the other hand, says that it has given the defense at least nine other documents relating to the Company 3 allegations. (ECF No. 496 at 43.)

[19] With respect to the defendant's argument that the government was reckless, "the Second Circuit has not specifically blessed the 'reckless disregard' standard, but neither has it declined to follow it." *Jordan*, 629 F. Supp. 3d at 54 n.1. In any event, the defendants have not shown that the government conducted the investigation recklessly.

pending before the Court. (*E.g.*, ECF No. 419 at 6–7; ECF No. 523 at 9–10.) Moreover, "speculation as to the government's motives" is not sufficient "where, as here, the government has responded with a specific rebuttal describing the reasons for the length of its investigation." *Scala*, 388 F. Supp. 2d at 401; *see also United States v. Mickens*, No. 20-258, 2021 WL 3136083, at *2 (2d Cir. July 26, 2021) ("Defendants point to no evidence suggesting that the reason for the Government's delay was improper . . . [f]or this reason, too, the District Court did not err in denying the motion for dismissal based on delay."); *cf. United States v. Gross*, 165 F. Supp. 2d 372, 384 (E.D.N.Y. 2001) (finding improper investigative delay where "the Government's failure to act was evidenced by large gaps of time with no case activity whatsoever," the case consistently shifted to different prosecutors, and there was sworn testimony that "the case . . . had been ready for two years").[20]

III. Counts 4–9: Financial Institution Fraud Charges

Counts 4 through 9 of the indictment charge Huawei — with Meng and Skycom (Counts 4, 6, 7, and 9) and the sealed defendants (Counts 5 and 8) — with wire fraud and bank fraud and conspiracies to commit wire fraud and bank fraud.[21] (ECF No. 126 ¶¶ 99–110.) The defendants do not deny that Counts 4 through 9 tracks the statutory language of the wire and bank fraud statutes. Rather, they argue that dismissal is required because the charges impermissibly allege

[20] "[B]ecause the Court has already determined that [the defendants] have not established substantial prejudice resulting from the purported delay, a hearing to . . . establish reckless or intentional conduct on the part of the Government would be of no legal consequence even if successful." *Jordan*, 629 F. Supp. 3d at 57; *accord United States v. Laureano*, No. 22-CR-58, 2023 WL 4156930, at *5 (S.D.N.Y. June 23, 2023).

[21] A defendant commits bank fraud in violation of 18 U.S.C. § 1344 when he, "executes, or attempts to execute, a scheme or artifice— (1) to defraud a financial institution; or (2) to obtain any of the moneys, funds, credits, assets, securities, or other property owned by, or under the custody or control of, a financial institution, by means of false or fraudulent pretenses, representations, or promises." 18 U.S.C. § 1349 criminalizes conspiring to commit bank fraud.

extraterritorial conduct and rely on a right-to-control theory of fraud that the Supreme Court invalidated in *Ciminelli v. United States*, 598 U.S. 306 (2023). (ECF No. 474-3 at 12.)

The government responds that the charges are based on "two criminal schemes, both of which were designed to obtain the financial institutions' funds in the form of dollar-clearing transactions." (ECF No. 496 at 50.) The first scheme concerns Huawei's "operation of Skycom as an unofficial subsidiary to obtain otherwise prohibited U.S.-origin goods, technology and services, including banking services, for [Huawei's] Iran-based business while concealing the link to [Huawei].'" (*Id.* (quoting ECF No. 126 ¶ 70).) The indictment alleges that beginning in July 2007, Huawei "repeatedly misrepresented to . . . various victim financial institutions" that its business in Iran "did not violate applicable U.S. law," including the ITSR, when in fact it did. (ECF No. 126 ¶ 71.) Had the four Financial Institutions known about these violations, "they would have reevaluated their banking relationships" with Huawei, "including their provision of U.S.-dollar and Euro clearing services." (*Id.*) The indictment also alleges that Huawei "repeatedly misrepresented to Financial Institution 1" that it "would not use Financial Institution 1 and its affiliates to process any transactions" related to its Iran-based business, when in reality it used "Subsidiary 1 and other financial institutions operating in the United States to process U.S.-dollar clearing transactions involving millions of dollars" related to Huawei's Iran-based business. (*Id.* ¶ 72.)

The second scheme relates to the defendants' conduct after "Financial Institution 1's decision to terminate its banking relationship" with Huawei. (ECF No. 496 at 51.) According to the indictment, after Financial Institution 1 ended the banking relationship, Huawei "took steps to secure and expand its banking relationships with other financial institutions, including Financial Institution 4." (*Id.*) The indictment charges that Huawei "made material

misrepresentations to . . . Subsidiary 4, among other financial institutions, regarding the reason for the termination of its relationship with Financial Institution 1," and that "[b]ased in part on these false representations and omissions," Subsidiary 4 "undertook to expand its banking relationship" with Huawei. (ECF No. 126 ¶¶ 84–85.) By "avoiding the termination of [its] relationship" with Financial Institution 4 and Subsidiary 4, Huawei "received income indirectly in the form of cost savings and the value of continued banking services, the proceeds of which income were used to operate and grow [its] business." (*Id.* ¶ 86.) The indictment alleges that at least part of each scheme took place in this district. (*Id.* ¶¶ 72, 84.)

a. *Ciminelli*

Louis Ciminelli was convicted of wire fraud and wire fraud conspiracy based on the "right-to-control theory" of fraud; under that theory, a "'cognizable harm occurs where the defendant's scheme denies the victim the right to control its assets by depriving it of information necessary to make discretionary economic decisions.'" 598 U.S. at 313 (quoting *United States v. Binday*, 804 F.3d 558, 570 (2d Cir. 2015) (alterations omitted)). The Supreme Court reversed the conviction. The Court concluded that the right-to-control theory could not "be squared with the text of the federal fraud statutes, which are 'limited in scope to the protection of property rights,'" that the theory was "inconsistent with the structure and history of the federal fraud statutes," and that it impermissibly "expand[ed] federal jurisdiction without statutory authorization" because "treating information as the protected interest [means] almost any deceptive act could be criminal." *Id.* at 314–15. The Court held that the "federal fraud statutes" — in that case, the mail and wire fraud statutes — "criminalize only schemes to deprive people of traditional property interests:" in other words, money or property. *Id.* at 309 (citing *Cleveland v. United States*, 531 U.S. 12, 24 (2000)). Courts in this circuit have found that *Ciminelli* applies

to the bank fraud statute. *See United States v. An*, 733 F. Supp. 3d 77, 91 (E.D.N.Y. 2024); *Bankman-Fried*, 680 F. Supp. 3d at 305; *United States, v. Mansouri*, No. 22-CR-34, 2023 WL 8430239, at *2–3 (W.D.N.Y. Dec. 5, 2023).

Huawei argues that Counts 4 through 9 "are based on the now-abrogated right-to-control theory" because the indictment "does not allege or identify *any* traditional property interest that Huawei allegedly sought to obtain or to deprive the banks of." (ECF No. 474-3 at 12.) Rather, the defendants say, the indictment alleges that "if the banks had known the truth, they would have reevaluated their banking relationship with Huawei," a harm that is "unmistakably a right-to-control theory." (*Id.* at 12–13.)

Relying on *Shaw v. United States*, 580 U.S. 63 (2016), the government responds that a traditional property interest under the bank fraud statute includes "a financial institution's property rights in a bank account." (ECF No. 496 at 54.) The government argues that Huawei "engaged in a scheme to access funds under the control of the Victim Financial Institutions" by "seeking continued access to U.S.-dollar clearing and other financial services," allegations that support the bank fraud and wire fraud charges. (*Id.* at 56.)

As an initial matter, it is not clear that *Ciminelli* applies at the motion to dismiss stage. In his concurring opinion, Justice Alito noted that he did "not understand the Court's opinion to address . . . the indictment's sufficiency . . . ." 598 U.S. at 317 (Alito, J. concurring). At least three courts in this circuit have held that it does not. *Xu*, 2024 WL 1332548, at *2 n.1 (S.D.N.Y. Mar. 28, 2024) ("*Ciminelli* is about instructional error, not the sufficiency of an indictment."); *accord, An*, 733 F. Supp. 3d at 91; *United States v. Lou*, No. 24-CR-99, ECF No. 25 at 6 (E.D.N.Y. Feb. 28, 2025).[22]

[22] In *United States v. Aiello*, 118 F.4th 291 (2d Cir. 2024), the Second Circuit vacated the defendant's wire fraud and wire fraud conspiracy trial convictions, observing that "[b]ecause the operative

Regardless, *Ciminelli* is not a reason to dismiss Counts 4 through 9. As the Supreme Court explained in *Shaw*, "a plan to deprive a bank of money in a customer's deposit account is a plan to deprive the bank of 'something of value' within the meaning of the bank fraud statute;" the government "need not prove that the defendant intended that the bank ultimately suffer monetary loss." 580 U.S. at 71–72. When the victim of the fraud is a financial institution, the Supreme Court has implied that this logic extends to the "analogous" mail and wire fraud statutes. *See id.* at 67–68 (citing *Carpenter v. United States*, 484 U.S. 19, 26–27 (1987)).

As the government points out, courts in this circuit have found that indictments which do not rely "*entirely* on an informational harm theory" survive *Ciminelli* challenges on a motion to dismiss. *An*, 733 F. Supp. 3d at 92; *see also Bankman-Fried*, 680 F. Supp. 3d at 305 ("*Ciminelli* is inapposite because the S5 Indictment alleges that the defendant conspired to induce a bank to open an account, which was used to receive FTX customer deposits and from which the defendant and his co-conspirators 'regularly took money' from the bank's custody."); *United States v. Motovich*, No. 21-CR-497, 2024 WL 2943960, at *6 (E.D.N.Y. June 11, 2024) (denying motion to dismiss bank fraud charges where the indictment "alleg[ed] the object of Defendants' bank fraud offenses was bank property, i.e., funds in the Shell Company Bank Accounts").

These decisions stand for the well-established rule that an indictment that "tracks the statutory language of [a bank or wire fraud statute] and sufficiently alleges that the defendant conspired to obtain 'money or property' in violation of the statute" will survive a motion to dismiss. *Bankman-Fried*, 680 F. Supp. 3d at 305; *see also United States v. Aronov*, No. 19-CR-408, 2024 WL 554577, at *4 (E.D.N.Y. Feb. 12, 2024) (denying a motion to dismiss wire fraud

indictment relied only on the right-to-control theory, to proceed to a second trial on a traditional property theory, the government would likely have to obtain another superseding indictment." *Id.* at 302 n.2. In that case, the government relied explicitly on the right-to-control theory at trial.

charges where "[t]he Indictment . . . alleges that Defendants schemed to defraud others of money and real property . . . rather than solely depriving the victims of valuable economic information needed to make discretionary economic decisions" (citation and internal quotations omitted)); *United States v. Pierre*, No. 22-CR-19, 2023 WL 4493511, at *15 (S.D.N.Y. July 12, 2023) (denying a motion to dismiss based on *Ciminelli* where "the Indictments do not mention the right to control, nor does the Government rely on the right to control theory in its briefing").

The indictment in this case charges Huawei and its co-conspirators with conspiring to defraud the Financial Institutions to "obtain moneys, funds, credits and other property." (ECF No. 126 ¶¶ 100, 102, 106, 108). Similarly, the wire fraud conspiracy and substantive wire fraud charges allege that Huawei intended to "obtain money and property" from the Financial Institutions. (*Id.* ¶¶ 104, 110.) Moreover, the factual allegations include "U.S.-dollar clearing transactions" and other "continued banking services," traditional property interests that are recognized under *Shaw*. (*Id.* ¶¶ 72, 86; ECF No. 496 at 56–57.)[23] Because the government does not rely "*entirely* on an informational harm theory," Counts 4 through 9 — which track the bank and wire fraud statutes — survive a motion to dismiss. *An*, 733 F. Supp. 3d at 92.

Huawei claims that the cases are distinguishable because "they involve schemes to obtain money the bank held *for a third party*." (ECF No. 515 at 30 (discussing *Bankman-Fried*, 680 F.

[23] Huawei argues that money moved by a bank as a part of a dollar-clearing transaction cannot constitute a property interest under *Ciminelli* because "[c]learing transactions are an entirely mechanical function" and do not deprive financial institutions "of an opportunity to profit from the funds involved" in the transaction. (ECF No. 515 at 30 n.14 (quoting *Jesner v. Arab Bank*, PLC, 584 U.S. 241, 250 (2018)).) Under *Shaw*, however,"[w]hen a customer deposits funds, the bank ordinarily becomes the owner of the funds," even where "the contract between the customer and the bank provides that the customer retains ownership of the funds and the bank merely assumes possession." 580 U.S. at 66. Thus, banks can possess a client's funds in dollar clearing, even if only for a short time. In any event, the indictment also alleges that Huawei defrauded and conspired to defraud the Financial Institutions out of money and other financial services.

Supp. 3d at 305; *Motovich*, 2024 WL 2943960, at *3; *Mansouri*, 2023 WL 8430239, at *1).)[24] Judge Matsumoto rejected a similar argument in *An*, where the defendants argued that "the alleged scheme could not have 'deprived' the victim banks of any property interest because the scheme only resulted in the [defendants] depositing their own money" with the banks. 733 F. Supp. 3d at 93. Judge Matsumoto acknowledged that the "presumed profit to the bank from maintaining and protecting the funds in the customer accounts is a property interest" under *Shaw*, and observed that "a scheme to defraud requires 'neither a showing of ultimate financial loss nor a showing of intent to cause financial loss.'" *Id.* at 93–94 (quoting *Shaw*, 580 U.S. at 67). Further, "even if it were established at trial that all the relevant funds and accounts belonged to" the defendants, "that would not necessarily require dismissal because the victim banks generally would have had ownership or at least possessory interests in the deposited funds and presumably would have profited from the accounts." *Id.* at 94. In any event, the Court finds, as Judge Matsumoto did, that the questions of who possessed the funds and "nature of the contractual relationships between the [defendants] and banks" are "factual issue[s] that must be resolved at trial." *Id.*[25]

[24] According to Huawei, this case has "more in common with *United States v. Nejad*, another Iran-sanctions/dollar-clearing case . . . in which the government *openly acknowledged* that its charge of fraud on the dollar-clearing banks was predicated on a right-to-control theory." (ECF No. 515 at 25–26.) *Nejad* is easily distinguishable. There, "the government opposed the defendant's motion to dismiss by explicitly characterizing its case as a right-to-control case." (*Id.* at 26.)

[25] There is no basis, as Huawei argues, for the Court to "order disclosure of the relevant portions of the legal instructions provided to the grand jury—or at least review them *in camera*—to determine whether . . . the right-to-control theory was . . . charged." (ECF No. 515 at 28.) "[A] defendant seeking disclosure of grand jury minutes has the burden of showing a 'particularized need' that outweighs the default 'need for secrecy' in grand jury deliberations." *United States v. Phillips*, 2023 WL 6812286, at *2 (S.D.N.Y. Oct. 16, 2023) (quoting *United States v. Forde*, 740 F. Supp. 2d 406, 413 (S.D.N.Y. 2010)); *see also United States v. Alexander*, 860 F.2d 508, 513 (2d Cir. 1988). Huawei's "premise is faulty [because] the indictment is not deficient" and "in any event, the Government need not provide the jury with legal instructions at all." *United States v. Perez*, No. 23-CR-99, 2025 WL 41612, at *5 (S.D.N.Y. Jan. 7, 2025) (citation omitted).

For these reasons, the defendant's motion to dismiss the case based on *Ciminelli* is denied.[26]

b. Extraterritoriality

Next, Huawei argues that Counts 4, 6, 7, and 9 must be dismissed because they are impermissibly extraterritorial and do not allege domestic application of the wire and bank fraud statutes. (ECF No. 474-3 at 15.) Huawei asserts that the press statements to which the indictment refers were "retransmitted by *others* to the United States;" that the dollar-clearing transactions were "facially incidental to the alleged scheme" because "Huawei could have accomplished the transactions in question without causing the use of any domestic wires;" and that any false statements that Huawei made to the Financial Institutions were "made outside the United States to individuals and entities outside the United States." (*Id.* at 19–21.)

Huawei also contends that that the bank fraud charges do not "allege that *any* conduct relevant to the scheme occurred domestically;" rather, the "crux of the alleged scheme" — the 2013 conversation between Meng and Financial Institution 1 — "took place abroad" and involved foreign companies and employees. (*Id.* at 22–23.) Further, Huawei argues that the dollar-clearing transactions that Subsidiary 1 processed were not "'core component[s]' of the scheme" and therefore do not qualify as domestic conduct. (*Id.* at 24 (quoting *Bascunan v. Elsaca*, 927 F.3d 108, 121, 124 (2d Cir. 2019)).)

The government responds that Huawei's "argument depends on the evidence to be presented at trial and thus is premature." (ECF No. 496 at 58.) Regardless, the government

[26] Huawei argues that if the Court does not dismiss Counts 4 through 9 it "should order the government to provide particulars concerning the money or property that was the object of Huawei's alleged schemes." (ECF No. 515 at 30.) The Court will address that in deciding the defendants' motion for a bill of particulars. (ECF No. 533; ECF No. 533-1 at 13.)

argues, "the heart of the fraudulent scheme was the continuing use of U.S.-dollar clearing services through U.S. banks." (*Id.* at 61.) The government also cites the allegations that Huawei made statements to the press and Financial Institutions "regarding [its] compliance with the U.S. sanctions regime," transmitted "domestic wires . . . to process millions of dollars in Iran-related business activity," and, through its employees, falsely testified to Congress and misrepresented its compliance with federal law to a principal of Subsidiary 4. (*Id.* at 61–62.)

It is well-established that the wire and bank fraud statutes at issue do not apply extraterritorially. *Bascunan*, 927 F.3d at 121, 124 (concluding that the "mail and wire fraud statutes do not indicate an extraterritorial reach" and that "the bank fraud statute does not purport to apply to extraterritorial conduct"). However, the question of whether a charge is impermissibly extraterritorial "typically is assessed after a full presentation of the evidence at trial." *Bankman-Fried*, 680 F. Supp. 3d at 309. Nonetheless, courts evaluating extraterritoriality claims on a Rule 12(b) motion have consistently found that an indictment which alleges domestic application of a criminal statute survives dismissal. *E.g.*, *id.*; *Chang*, No. 18-CR-681, 2024 WL 2817494, at *7 (E.D.N.Y. May 31, 2024); *United States v. Halkbank*, No. 15-CR-867, 2020 WL 5849512, at *7 (S.D.N.Y. Oct. 1, 2020), *aff'd sub nom. United States v. Turkiye Halk Bankasi A.S.*, 16 F.4th 336 (2d Cir. 2021), *aff'd in part, vacated in part, remanded*, 598 U.S. 264 (2023). In reaching this determination, "[t]here is no requirement that the indictment contain allegations of defendant's presence in the United States, actual communications into or out of the United States, or transaction of business within the United States." *United States v. Mostafa*, 965 F. Supp. 2d 451, 459 (S.D.N.Y. 2013). Rather, "the determinative issue is whether defendant's actions were calculated to harm American citizens and interests." *Id.*; *see also Prime Int'l*

Trading, Ltd. v. BP P.L.C., 937 F.3d 94, 102 (2d Cir. 2019) ("[C]ourts must evaluate whether the domestic activity involved implicates the 'focus' of the statute.").

The question of extraterritoriality should be decided after a full presentation of the evidence at trial. *United States v. Karony*, No. 23-CR-433, 2025 WL 1149473, at *1 (E.D.N.Y. Apr. 18, 2025) ("[A]s with any merits question, the government is 'entitled to put on its evidence' about the domestic (or non-domestic) application of the statute, and the defendant is entitled to challenge that evidence 'both on a Rule 29 motion and before the jury.'" (quoting *Phillips*, 690 F. Supp. 3d at 284)); *see also United States v. Prado*, 933 F.3d 121, 138 (2d Cir. 2019) (explaining that whether an indictment charges domestic or extraterritorial conduct "is a merits question"). At this stage of the proceedings, Counts 4, 6, 7, and 9 adequately allege a domestic application of the wire and bank fraud statutes. The counts track the relevant statutory language. Counts 4 and 7 allege that Huawei conspired to execute and executed "a scheme and artifice to defraud . . . Subsidiary 1." (ECF No. 126 ¶¶ 100, 106.) Counts 6 and 9 allege "a scheme and artifice to defraud the Victim Institutions," which encompasses their American subsidiaries. (*Id.* ¶¶ 71, 104, 110.) The indictment also charges that Huawei made false statements to the Financial Institutions (including their American subsidiaries) about the company's compliance with federal law; issued press releases responding to reports by American media or media with a significant United States footprint; met with and made misrepresentations to Subsidiary 4 employees; and availed itself of U.S.-dollar clearing transactions and other financial services with the Financial Institutions. (*Id.* ¶¶ 64, 71, 73–75, 76–77, 84–86.) The indictment sufficiently alleges conduct in furtherance of fraudulent schemes "calculated to harm American citizens and interests." *Mostafa*, 965 F. Supp. 2d at 459.

Huawei does not cite, and the Court has not found, any decisions in this circuit granting a motion to dismiss an indictment on extraterritoriality grounds. *See Bankman-Fried*, 680 F. Supp. 3d at 309 ("[T]he defendant has not identified and the Court is not aware of any case in this district where an indictment has been dismissed on extraterritoriality grounds at the motion to dismiss stage."). Huawei cites one out-of-circuit case, *United States v. Sidorenko*, 102 F. Supp. 3d 1124 (N.D. Cal. 2015), but *Sidorenko* is neither binding nor analogous to the indictment here. There, the court dismissed the indictment on due process grounds because there was "nothing in the Indictment to support the proposition that any of the Defendants knew that the conduct alleged even involved the United States" and the government could not satisfy the Ninth Circuit's domestic nexus test. *Id.* at 1132–33. The indictment in this case sufficiently alleges conduct in and affecting the United States. Accordingly, the Court denies Huawei's motion to dismiss Counts 4, 6, 7, and 9 on extraterritoriality grounds.

IV. Count 10: *Klein* Conspiracy

Count 10 charges Huawei and Skycom with a conspiracy to defraud the United States, in violation of 18 U.S.C. § 371. (ECF No. 126 ¶¶ 111–13.) Under Section 371, it is illegal to "conspire either to commit any offense against the United States, or to defraud the United States, or any agency thereof in any manner or for any purpose." 18 U.S.C. § 371. The Second Circuit has long held that Section 371 "not only includes cheating the Government out of property or money, but 'also means to interfere with or obstruct one of its lawful government functions by deceit, craft or trickery.'" *United States v. Klein*, 247 F.2d 908, 916 (2d Cir. 1957) (quoting *Hammerschmidt v. United States*, 265 U.S. 182, 188 (1924)). A conspiracy to interfere with or obstruct the functioning of a federal agency — a "*Klein* conspiracy" — violates Section 371. *See United States v. Atilla*, 966 F.3d 118, 131 (2d Cir. 2020); *United States v. Stewart*, 590 F.3d 93, 108–09 (2d Cir. 2009); *United States v. Ballistrea*, 101 F.3d 827, 832–33 (2d Cir. 1996).

The indictment alleges that Huawei and Skycom "conspire[d] to defraud the United States by impairing, impeding, obstructing and defeating, through deceitful and dishonest means, the lawful governmental functions and operations of OFAC . . . in the enforcement of economic sanctions laws and regulations . . . and the issuance . . . of appropriate licenses relating to the provision of financial services." (*Id.* ¶ 112.) The indictment lists nine "overt acts" Huawei and Skycom undertook in furtherance of this conspiracy:

(1) On July 11, 2007, a Huawei employee told FBI agents that Huawei "did not conduct any activity in violation of U.S. export laws . . . operated in compliance with all U.S. export laws . . . had not dealt directly with any Iranian company" and that he believed Huawei "sold equipment to a third party, possibly in Egypt, which in turn sold the equipment to Iran."

(2) On September 13, 2012, the Senior Vice President testified before Congress that Huawei's business in Iran "had not 'violated any laws and regulations including sanction-related requirements.'"

(3) On September 17, 2012, Meng met with a "principal" of Subsidiary 4 in New York and stated that Huawei and its "global affiliates" did not violate any applicable United States law.

(4) On July 24, 2013, Skycom "caused . . . Subsidiary 1 to process a U.S.-dollar clearing transaction of $52,791.08."

(5) On July 24, 2013, Skycom "caused a bank located in the Eastern District of New York," identified as "Bank 1" to "process a U.S.-dollar clearing transaction of $94,829.82."

(6) On August 20, 2013, Skycom "caused Bank 1 to process a U.S.-dollar clearing transaction of $14,835.22."

(7) On August 28, 2013, Skycom "caused Bank 1 to process a U.S.-dollar clearing transaction of $32,663.10."

(8) On April 11, 2014, Skycom "caused a bank located in the United States," identified as "Bank 2" to "process a U.S.-dollar clearing transaction of $118,842.45."

(9) In April 2018, Huawei "made efforts to move an employee . . . with knowledge about [its] Iran-based business to the PRC, and beyond the jurisdiction of the U.S. government."

(*Id.* ¶ 113.)

Huawei argues that, after *Ciminelli*, "[a]n interpretation of § 371 that makes it a crime to 'defraud' the United States without any intent to obtain money or property from the United States . . . cannot be squared with the Supreme Court's . . . understanding of what fraud is." (ECF No. 474-4 at 17.) In other words, Huawei argues that *Ciminelli*'s declaration that the "federal fraud statutes" criminalize "only schemes to deprive people of traditional property interests," 598 U.S. at 309, 314–15 (citing *Cleveland*, 531 U.S. at 24), also applies to a charge under Section 371.[27]

Huawei acknowledges, as it must, that the Second Circuit declined to overrule the *Klein* doctrine, despite reservations about its continued validity. *United States v. Coplan*, 703 F.3d 46, 61–62 (2d Cir. 2012) ("Although the defendants argue forcefully on appeal that we should . . . 'pare' the body of § 371 precedent 'down to its core,' such arguments are properly directed to a higher authority . . . we are bound to follow the dictates of Supreme Court precedents, no matter how persuasive we find the arguments for breaking loose from the moorings of established judicial norms by 'paring' a statute." (internal citations omitted)). District courts are "bound to follow controlling Second Circuit precedent unless that precedent is overruled or reversed." *United States v. Kelly*, 609 F. Supp. 3d 85, 131 (E.D.N.Y. 2022) (quoting *Unicorn Bulk Traders Ltd. v. Fortune Mar. Enters., Inc.*, No. 08-CV-9710, 2009 WL 125751, at *2 (S.D.N.Y. Jan. 20, 2009)), *aff'd*, No. 22-1481, 2025 WL 466673 (2d Cir. Feb. 12, 2025).

In any event, the Court does not agree that the Supreme Court, by its general observation that "[t]he right-to-control theory cannot be squared with the text of the federal fraud statutes,"

[27] Huawei also argues that a *Klein* conspiracy must allege interference with a specific government act, "not merely general agency operations," and that the statute is unconstitutionally vague. (ECF No. 474-4 at 17–20.) Huawei concedes, however, that the Second Circuit rejected these arguments in *Atilla*, 966 F.3d 118, a decision that the Court must follow. (*Id.* at 18, 19–20.)

Ciminelli, 598 U.S. at 314, meant to redefine the reach of every fraud statute, including Section 371, or to overrule *Klein*. Unlike the wire and mail fraud statutes at issue in *Ciminelli*, a Section 371 conspiracy encompasses efforts to "defraud the United States, or any agency thereof in any manner or for any purpose." 18 U.S.C. § 371. In *Ciminelli*, the Supreme Court stated that it has "consistently understood" the mail and wire fraud statutes' "'money or property' requirement as limiting the 'scheme or artifice to defraud' element" in those statutes. 598 U.S. at 312.

By contrast, the Second Circuit has explained that "the term 'defraud' in § 371 'is not confined to fraud as that term has been defined in the common law,'" *Atilla*, 966 F.3d at 130 (quoting *Coplan*, 703 F.3d at 61), at least partly because Section 371 "is designed to protect the integrity of the United States and its agencies," *Ballistrea*, 101 F.3d at 831 (quoting *United States v. Nersesian*, 824 F.2d 1294, 1313 (2d Cir. 1987)). In evaluating federal fraud statutes, judges in this circuit have reached the same conclusion. *Chang*, 2024 WL 2817494, at *5 ("[W]hile *Ciminelli* discussed the 'federal fraud statutes,' the case's discussion was limited to the mail and wire fraud statutes, with no discussion of the securities fraud statutes."); *United States v. Lingat*, No. 21-CR-573, 2024 WL 3594565, at *5 (S.D.N.Y. July 30, 2024) (finding that "the series of Supreme Court cases paring down the reach of certain other federal statutes" did not compel a finding that the *Klein* doctrine must be overruled). Accordingly, the motion to dismiss Count 10 of the indictment is denied.

V. Counts 11 and 12: IEEPA Charges

Counts 11 and 12 charge Huawei and Skycom with violating and conspiring to violate the IEEPA. (ECF No. 126 ¶¶ 114–120.) The indictment alleges that Huawei and Skycom "conspire[d] to cause" and "cause[d]" the "export, reexport, sale and supply . . . [of] banking and other financial services from the United States to Iran and the Government of Iran, without having first obtained the required OFAC license." (*Id.* ¶¶ 118, 120.) According to the

government, the defendants violated the ITSR,[28] which prohibited the "exportation, reexportation, sale or supply from the United States, or by a U.S. person . . . of any goods, technology or services," to Iran or its government, as well as "[a]ny transaction by a U.S. person" that involved "goods, technology or services for exportation, reexportation, sale or supply" to Iran or its government or that "evaded or avoided, had the purpose of evading or avoiding, attempted to violate, or caused a violation of any of the prohibitions in the ITSR." (*Id.* ¶ 116.)

Huawei argues that Counts 11 and 12 should be dismissed because they fail to state an offense and they violate due process. These arguments are without merit.

a. Failure to State an Offense

As explained above, while "a federal indictment can be challenged on the ground that it fails to allege a crime within the terms of the applicable statute," *Aleynikov*, 676 F.3d at 75–76 (internal quotation marks and citations omitted), an indictment "need do little more than to track the language of the statute charged and state the time and place (in approximate terms) of the alleged crime," *Stringer*, 730 F.3d at 124 (internal quotation marks and citation omitted). *See also United States v. Budovsky*, No. 13-CR-368, 2015 WL 5602853, at *3 (S.D.N.Y. Sept. 23, 2015) ("[T]he indictment need only allege the 'core of criminality' the Government intends to prove at trial, since the indictment is 'read . . . to include facts which are necessarily implied by the specific allegations made.'" (quoting *United States v. Rigas*, 490 F.3d 208, 228–29 (2d Cir. 2007)).

[28] The ITSR was promulgated by OFAC pursuant to the IEEPA.

Huawei concedes that the language of Counts 11 and 12 "tracks [the] ITSR." (ECF No. 474-4 at 9.)[29] Nonetheless, Huawei argues that "the government's bill of particulars response . . . shows that the government accepts that the alleged transactions" underlying the charges "did not involve any 'transfer of funds to Iran.'" (*Id.*) Huawei asserts that none of the dollar-clearing transactions were "sent to or from a bank account in Iran [or] passed through an account in Iran," and that dollar-clearing "was a service that U.S. banks provided to overseas banks, permitting overseas-sending banks and overseas-receiving banks to transfer U.S. dollars from one to the other." (*Id.*) Because "the parties to the payments alleged here were Huawei . . . Skycom . . . or other non-Iranian parties," Huawei argues, there "was no 'benefit' from the dollar-clearing services to Iran." (*Id.* at 10.) Huawei asserts that the indictment does not state a claim under the IEEPA because it does not allege that the dollar-clearing transactions were supplied to Iran or its government. (*Id.* at 9–10.)

The "execution on behalf of others of money transfers from the United States to Iran is a 'service' under the terms of the" ITSR. *United States v. Homa Int'l Trading Corp.*, 387 F.3d 144, 146 (2d Cir. 2004). In addition to proscribing the direct provision of services, ITSR Section 204 forbids "indirectly" providing services to Iran or its government. 31 C.F.R. § 560.204. "[P]ursuant to the text of Section [204], a *service* is *indirectly* exported to Iran if it is performed outside Iran but the benefit of it is ultimately received by persons or entities in Iran." *United States v. Nejad*, No. 18-CR-224, 2019 WL 6702361, at *4 (S.D.N.Y. Dec. 6, 2019).

[29] ITSR Section 204 prohibits prohibits the supply "from the United States, or by a United States person" of any "services to Iran or the Government of Iran." 31 C.F.R. § 560.204. Pursuant to Section 427 of the ITSR, this prohibition includes the "transfer of funds, directly or indirectly, from the United States or by a U.S. person, wherever located, to Iran or the Government of Iran," as well as the "provision, directly or indirectly, to Iran or the Government of Iran of … banking services." 31 C.F.R. § 560.427(a).

Counts 11 and 12 allege that Huawei and Skycom sought to "export . . . directly and indirectly . . . banking and other financial services from the United States to Iran and the Government of Iran," in violation of the ISTR. (ECF No. 126 ¶¶ 118, 120.) According to the indictment, Skycom was a Hong Kong corporation that Huawei "operated . . . as an unofficial subsidiary to obtain otherwise prohibited . . . banking services," for Huawei's "Iran-based business." (*Id.* ¶¶ 4, 70.) The indictment also alleges that Skycom "employed in Iran at least one U.S. citizen" and that Financial Institution 1 and Subsidiary 1 "cleared more than $100 million worth of transactions" related to Skycom "through the United States." (*Id.* ¶¶ 64, 70.)

Regardless of whether Skycom was located or incorporated in Iran, the indictment satisfactorily alleges that the company operated as Huawei's Iranian subsidiary and "ultimately stood to benefit, in a roundabout way, from the processing of these fund transfers." *Nejad*, 2019 WL 6702361, at *4.[30] These allegations are sufficient to state an offense under the ITSR. Whether the dollar-clearing transactions "were processed by non-Iranian banks on behalf of non-Iranian customers" and services were never actually exported "to Iran," (ECF No. 515 at 34–35), are factual questions for a jury.

b. Vagueness

Finally, Huawei moves to dismiss Counts 11 and 12 because the IEEPA did not provide fair warning that Huawei "could be subject to criminal liability as a non-U.S. person . . . when [its] banks opted to route the payments through the United States." (ECF No. 474-4 at 10.) The Supreme Court has explained that there are "three related manifestations" of fair warning

[30] Huawei distinguishes *Nejad* because the "payments were transferred through shell companies for an Iranian-incorporated entity," whereas neither Huawei nor Skycom are Iranian. (ECF No. 474-4 at 10 (citation and internal quotations omitted).) In *Nejad*, however, the benefit of the services was received in Iran; here, the government alleges that Huawei "use[d] the U.S. banking system to further its business interests in Iran" through Skycom. (ECF No. 496 at 67.)

challenges: the vagueness doctrine, the rule of lenity, and the novel construction of a statute. *United States v. Lanier*, 520 U.S. 259, 266–67 (1997). Huawei brings a challenge under the vagueness doctrine. (*See* ECF No. 515 at 35–36.)

The vagueness doctrine "requires that a penal statute define the criminal offense with sufficient definiteness that ordinary people can understand what conduct is prohibited and in a manner that does not encourage arbitrary and discriminatory enforcement." *United States v. Rybicki*, 354 F.3d 124, 129 (2d Cir. 2003) (quoting *Kolender v. Lawson*, 461 U.S. 352, 357 (1983)). "[V]agueness challenges that do not involve the First Amendment must be examined in light of the specific facts of the case at hand and not with regard to the statute's facial validity." *United States v. Nadi*, 996 F.2d 548, 550 (2d Cir. 1993); *see also United States v. Coiro*, 922 F.2d 1008, 1017 (2d Cir. 1991) ("In the absence of first amendment considerations, vagueness challenges must be considered in light of the facts of the particular case."). Before a court can resolve an as-applied vagueness challenge, "it must be clear what the defendant did." *Phillips*, 690 F. Supp. 3d at 292 (quoting *Raniere*, 384 F. Supp. 3d at 320–21). Accordingly, a court should deny as premature a motion to dismiss on vagueness grounds when further factual development is required. *E.g.*, *United States v. Shea*, No. 20-CR-412, 2022 WL 1443918, at *5 (S.D.N.Y. May 6, 2022) ("Because it is assessing an as-applied challenge, the Court must determine what Shea did before determining whether the statute fairly apprised him that his conduct was prohibited."); *United States v. Avenatti*, 432 F. Supp. 3d 354, 366 (S.D.N.Y. 2020) (denying as premature an as-applied vagueness challenge on a motion to dismiss); *United States v. Hoskins*, 73 F. Supp. 3d 154, 166 (D. Conn. 2014) ("Defendant's . . . 'as applied' challenge will require a more expansive factual record to be developed at trial regarding the 'highly factual' nature of the alleged agency relationship."); *United States v. Milani*, 739 F. Supp. 216,

218 (S.D.N.Y. 1990) ("On the issue of whether the statute might be unconstitutional as applied in a particular case, we must await conclusion of the trial.").

Like the cases described above, Huawei's challenge is premature. Because it is not yet "clear what the defendant did," the Court cannot assess Huawei's as-applied vagueness challenge at this stage. *Phillips*, 690 F. Supp. 3d at 292 (quoting *Raniere*, 384 F. Supp. 3d at 320–21). Accordingly, Huawei's motion to dismiss Counts 11 and 12 is denied.[31]

CONCLUSION

For the foregoing reasons, the defendants' motion is denied.

SO ORDERED.

s/Ann M. Donnelly

ANN M. DONNELLY
United States District Judge

Dated: Brooklyn, New York
July 1, 2025

[31] Because the Court denies Huawei's motion to dismiss Counts 11 and 12, there is no basis to dismiss Count 15, which charges a money laundering conspiracy predicated on the same conduct. (ECF No. 126 ¶ 126.)