IN THE UNITED STATES COURT OF APPEALS
FOR THE FIFTH CIRCUIT

No. 16-11340

United States Court of Appeals
Fifth Circuit
FILED
March 1, 2018
Lyle W. Cayce
Clerk

UNITED STATES OF AMERICA,

Plaintiff - Appellee

v.

LENNON RAY BROWN,

Defendant - Appellant

Appeal from the United States District Court
for the Northern District of Texas

Before JOLLY, DENNIS, and ELROD, Circuit Judges.

JAMES L. DENNIS, Circuit Judge:

Lennon Ray Brown, a former Citibank employee, pleaded guilty to intentionally damaging a protected computer in violation of 18 U.S.C. § 1030(a)(5)(A) after temporarily disabling a portion of Citibank's network. He was sentenced to twenty-one months of incarceration followed by two years of supervised release. On appeal, Brown argues that his Guidelines range was improperly increased under U.S.S.G. § 2B1.1(b)(18)(A)(iii), which applies to conduct causing a "substantial disruption of a critical infrastructure." Because we conclude that Brown's conduct could not have had a serious impact on national economic security, we VACATE Brown's sentence and remand for resentencing.

I

Brown was a system specialist at Citibank's Global Control Center in Irving, Texas. On December 23, 2013, Brown was called into a meeting with his supervisors and presented with a formal "Performance Improvement Plan" based on accusations of poor work performance. Brown refused to participate in the plan. At 6:03 p.m., about an hour after leaving the meeting, Brown connected to Citibank's secure network and intentionally executed commands to disrupt network traffic through ten of Citibank's data routers, ultimately impacting nine. Brown's sabotage resulted in a loss of connectivity to some but not all of Citbank's North American data centers, campuses, call centers, and sixty-nine ATMs. He then left the building, informing a coworker that he would not be returning. The Global Control Center almost immediately received an automatic alert notifying it of the outage and promptly committed company resources to resolve the problem. By 10:17 p.m., Citibank had restored ninety percent of the lost connectivity, and by 4:21 a.m. the next morning had fully restored the network.

Brown pleaded guilty without a plea agreement to a one-count indictment charging him with intentional damage to a protected computer in violation of 18 U.S.C. § 1030(a)(5)(A), (c)(4)(A)(i)(I), and (c)(4)(B). Brown's Presentence Report (PSR) calculated a total offense level of twenty-three with a criminal history category of I, resulting in a Guidelines range of forty-six to fifty-seven months of incarceration. The PSR calculated Citibank's actual loss as $133,402, including $56,202 for increased phone calls to call centers from customers affected by the outage. The PSR also applied a six-level sentencing enhancement under § 2B1.1(b)(18)(A)(iii) for a violation of § 1030 that caused a "substantial disruption of a critical infrastructure," bringing the offense level to twenty. Under § 2B1.1(b)(18)(B), because § 2B1.1(b)(18)(A)(iii) applied, the

offense level was then increased to twenty-four, effectively an additional four-level increase.

Brown subsequently filed a sentencing memorandum, requesting a downward variance and disputing the loss calculations and other facts included in the PSR. Brown alleged that his offense level was erroneously calculated under the Guidelines and proposed an alternative calculation that, relevant to this appeal, eliminated the six-level enhancement and corresponding level increase under § 2B1.1(b)(18)(A)(iii) and (18)(B) and substituted a mutually exclusive four-level enhancement under § 2B1.1(b)(18)(A)(ii). In its response, the Government stated that Brown "appear[ed] to object to the loss figure [and] the 6 level increase pursuant to § 2B1.1(b)(18)(A)(iii) for a substantial disruption of a critical infrastructure." The Government contended that the § 2B1.1(b)(18)(A)(iii) enhancement was correctly applied because Brown "shut down nine (9) [of] CITI's routers, causing a substantial disruption to CITI's call centers, and deleting essential encryption in the ATM systems and Global Transaction systems."

At sentencing, the district court concluded that the $56,202 figure included in the PSR's loss calculation as the amount attributable to increased customer contacts with Citibank's call center was too speculative and thus determined that the total loss suffered was $77,200. This lowered Brown's Guidelines range to thirty-seven to forty-six months of incarceration. On the Government's request, the district court then addressed other objections implicit in Brown's sentencing memorandum, ruling that "[t]o the extent those were objections, they are overruled." Citing Brown's otherwise upstanding personal history, the district court found that Brown's conviction constituted aberrant conduct and downwardly departed under U.S.S.G. § 5K2.20, imposing a sentence of 21 months of incarceration followed by two years of supervised release.

Brown appeals, challenging only the application of the enhancements under U.S.S.G. § 2B1.1(b)(18)(A)(iii) and (18)(B) for "substantial disruption of a critical infrastructure."

II

We review a district court's interpretation and application of the Guidelines de novo. *United States v. Hernandez*, 876 F.3d 161, 164 (5th Cir. 2017). However, when a defendant fails to raise a claim below, we review for plain error only. *Puckett v. United States*, 556 U.S. 129, 134–35 (2009).

The Government argues that Brown failed to preserve his issue on appeal by not raising it before the district court and, consequently, his claim is subject to plain error review. In order to preserve an argument for appeal, it "must be raised to such a degree that the district court has an opportunity to rule on it." *United States v. Soza*, 874 F.3d 884, 889 (5th Cir. 2017) (quoting *Dallas Gas Partners, L.P. v. Prospect Energy Corp.*, 733 F.3d 148, 157 (5th Cir. 2013)). "The raising party must present the issue so that it places the opposing party and the court on notice that a new issue is being raised." *Id.* (quoting *Kelly v. Foti*, 77 F.3d 819, 823 (5th Cir. 1996)). The appellant need not cite directly to the provision at issue so long as his objection below offered the opposing party and district court a fair opportunity to respond to its contention that a sentencing enhancement should not apply. *United States v. Ocana*, 204 F.3d 585, 589 (5th Cir. 2000) (finding issue preserved for appeal where appellant "did not specifically cite to the USSG section which the PSR applied, [but] she did make a general objection that notified the court of her disagreement" with the challenged enhancement).

Brown's sentencing memorandum did not explicitly argue that his conduct did not amount to a substantial disruption of critical infrastructure. However, he did directly dispute the calculation of his Guidelines range,

proposing an alternative calculation that eliminated the enhancement under (18)(A)(iii) and substituted a different enhancement:

The base offense level, 2B 1.1 is	-6
Loss between 5,000.-101[,]000	-2
1030(a)(5)A	-4
There is no sophisticated means	0
Total	12

Brown's proposed calculation does not include an enhancement under (18)(A)(iii). Instead, it includes a four-level enhancement for "1030(a)(5)A." This amounts to an objection that his sentence should have been enhanced under § 2B.1.1(b)(18)(A)(ii), which imposes a four-level increase for offenses committed under this particular subsection of 18 U.S.C. § 1030. Notably, §§ 2B.1.1(b)(18)(A)(ii) and (18)(A)(iii) are mutually exclusive provisions, with the Guidelines instructing the court to apply the greater that applies. Thus, by stating that the court should apply § 2B.1.1(b)(18)(A)(ii) and not (18)(A)(iii), Brown effectively put the Government and the court on notice that he objected to the greater increase under § 2B.1.1(b)(18)(A)(iii).

The Government's response demonstrates that Brown's sentencing memorandum put it on notice of this particular argument. The Government acknowledged that Brown, by proposing this alternative Guidelines calculation, "appears to object to . . . the 6 level increase pursuant to U.S.S.G. § 2B1.1(b)(18)(A)(iii) for a substantial disruption of a critical infrastructure," and then rebutted that implicit objection. *See Ocana*, 204 F.3d at 589 (finding that written response from probation officer that specifically referenced the indirectly challenged enhancement demonstrated that the opposing party and district court were "clearly notified" of the objection). At sentencing, the district court then overruled this and any other implicit objection Brown raised "to the extent that they were made."

Though Brown could have raised his objection more explicitly and thoroughly below, we conclude that he presented both the Government and the district court the opportunity to address Brown's issue on appeal, and consequently sufficiently preserved this issue for our review. *Cf. United States v. Neal*, 578 F.3d 270, 272 (5th Cir. 2009) ("While Neal could certainly have been more clear and more persistent in raising an objection . . . we conclude that his actions were sufficient to preserve error.").

III

Under U.S.S.G. § 2B.1.1(b)(18)(A)(iii), a six-level increase is warranted if a defendant is convicted of an offense under 18 U.S.C. § 1030 "and the offense caused a substantial disruption of a critical infrastructure." Further, under § 2B.1.1(b)(18)(B), "if subdivision (A)(iii) applies, and the offense level is less than level 24," a court is instructed to "increase [his] level to 24."

The commentary to the 2015 Sentencing Guidelines defines "critical infrastructure" as "systems and assets vital to national defense, national security, economic security, public health or safety, or any combination of these matters." U.S. Sentencing Guidelines Manual § 2B1.1(b)(18) cmt. n.14 (U.S. Sentencing Comm'n 2015). The enumerated examples include public and private "financing and banking systems." *Id.* Neither the text of the Guidelines nor the commentary, however, defines what constitutes a "substantial disruption." Nor has this circuit—or any other for that matter—resolved this question.[1] Accordingly, we look to the text of the Guidelines themselves, the relevant commentary, and statutory origins of the sentencing provision to inform our analysis.

[1] In *United States v. Mitra*, 405 F.3d 492, 496–97 (7th Cir. 2005), apparently the only circuit court decision to address this sentencing provision (under its former numbering at U.S.S.G. § 2B1.1(b)(13)(A)(iii)), the Seventh Circuit held that a city's computer-based radio system for emergency communications was "critical infrastructure," but did not discuss what constitutes a "substantial disruption."

Other language in § 2B1.1 indicates what is *not* a substantial disruption. Under § 2B1.1(b)(18)(A)(i), a defendant is eligible for only a two-level increase for a § 1030 conviction that, inter alia, "involved a computer system used to maintain or operate a critical infrastructure." If, like Brown, a defendant is convicted under § 1030(a)(5)(A) for conduct involving such a computer system, then § 2B1.1(b)(18)(A)(ii) would apply instead, resulting in a four-level enhancement. This subsection of § 1030 criminalizes "knowingly caus[ing] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally caus[ing] damage without authorization, to a protected computer." 18 U.S.C. § 1030(a)(5)(A). Necessarily, then, one who knowingly causes the transmission of a command that intentionally causes damage to a protected computer system used to maintain a critical infrastructure is not, without more, eligible for the (b)(18)(A)(iii) increase, only a four level increase under subsection (ii). Only if the damage caused a "substantial disruption" of that critical infrastructure do we look to § 2B1.1(b)(18)(A)(iii).

In contrast, the Commentary discusses conduct that is more egregious than that which causes a "substantial disruption." U.S. Sentencing Guidelines Manual § 2B1.1(b)(18) cmt. n.20(B) (U.S. Sentencing Comm'n 2015). This portion of the commentary recommends an upward departure "in a case in which subsection (b)(18)(A)(iii) applies and the disruption to the critical infrastructure(s) is *so substantial as to have a debilitating impact* on national security, national economic security, [and/or] national public health or safety." *Id.* (emphasis added). "Substantial disruption," then, must exist somewhere between the conduct sufficient for enhancement under § 2B1.1(b)(18)(A)(ii) and that which warrants this upward departure for disruptions that have a debilitating impact.

The Commentary further directs readers to § 2B1.1(b)(18)(A)(iii)'s statutory origins. U.S. Sentencing Guidelines Manual § 2B.1.1(b)(18) cmt. background (U.S. Sentencing Comm'n 2015). It notes that "[s]ubsection (b)(18) implements the directive in section 225(b) of Public Law 107-296," also known as the Cyber Security Enhancement Act of 2002. *Id.*; *see* 6 U.S.C. § 145. This act is a subsection of the Homeland Security Act, which was enacted in response to the September 11, 2001 terrorist attacks. 6 U.S.C. § 101 *et seq*.; *see, e.g.*, H.R. REP. NO. 107-609(I), at 63–67 (2002), *as reprinted in* 2002 U.S.C.C.A.N. 1352, 1353–57. The Cyber Security Enhancement Act instructed the Sentencing Commission to ensure that the recommended sentences for offenses under 18 U.S.C. § 1030 take into account, among other factors, whether the offending conduct "involved a computer used by the government in furtherance of national defense, national security, or the administration of justice," "creat[ed] a threat to public health or safety," or "significantly interfer[ed] with or disrupt[ed] a critical infrastructure." 6 U.S.C. § 145(2)(B).

According to the Commentary, § 2B1.1(b)(18)(A)(iii)'s enhancement for a "substantial disruption of a critical infrastructure" implements this directive from Congress by imposing harsher sentencing recommendations for those offenses that could have a "serious impact" on "national security, national economic security, national public health or safety, or a combination of any of these matters." U.S. Sentencing Guidelines Manual § 2B.1.1(b)(18) cmt. background (U.S. Sentencing Comm'n 2015). In specifying how this provision satisfies the statutory directive, the Commentary here suggests a limiting principle: to determine whether § 2B1.1(b)(18)(A)(iii) can be applied to a particular defendant, a court must ask whether his conduct was that which could have a "serious impact" on "national security, national economic security, [and/or] national public health or safety." *Id.*

Using the Commentary to guide our analysis, Brown's conduct did not constitute a "substantial disruption of a critical infrastructure." There is no indication that Brown's conduct affecting a portion of Citibank's operations for a short period of time could have had a serious impact on national economic security. As a result of Brown's actions, Citibank suffered relatively minor financial losses[2] and was temporarily unable to optimally serve its customers. Neither of these harms threatened to disrupt the nation's economy, and, in light of Citibank's demonstrated ability to quickly resolve the disruption and mitigate in the interim, there is no other evidence that Brown's conduct had the potential to do so. Accordingly, we hold that the district court erred by applying an enhancement that we conclude is reserved for conduct that disrupts a critical infrastructure in a way that could have a serious impact on national economic security.

***

For these reasons, the sentence imposed by the district court is VACATED. The case is REMANDED for resentencing consistent with this ruling, with instructions to expedite proceedings in light of Brown's scheduled release from custody.

[2] Citibank is one of the world's largest banks with over $1.4 trillion in assets. CONSUMER FIN. PROT. BUREAU, *CFPB Takes Action Against Citibank For Student Loan Servicing Failures That Harmed Borrowers*, (Nov. 21, 2017), https://www.consumerfinance.gov/about-us/newsroom/cfpb-takes-action-against-citibank-student-loan-servicing-failures-harmed-borrowers/.