[DO NOT PUBLISH]

IN THE UNITED STATES COURT OF APPEALS

FOR THE ELEVENTH CIRCUIT

No. 17-13108
Non-Argument Calendar

D.C. Docket No. 0:16-cr-60238-JIC-1

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

versus

JONATHAN LEE EUBANKS,

Defendant-Appellant.

Appeal from the United States District Court
for the Southern District of Florida

(October 26, 2018)

Before WILLIAM PRYOR, ANDERSON, and JULIE CARNES, Circuit Judges.

PER CURIAM:

A jury convicted Defendant Jonathan Eubanks of intentionally causing damage without authorization to a protected computer, use of unauthorized access devices, and three counts of aggravated identity theft. The district court sentenced Defendant to 84 months' imprisonment. Defendant now appeals, challenging the sufficiency of the evidence as to one of his aggravated identity theft convictions. He also argues that his sentence is procedurally and substantively unreasonable. After careful review, we affirm.

I. BACKGROUND

A. Facts[1]

Navarro Security ("Navarro") is a company that provides security services for gated communities, individuals, and businesses. In October 2012, Navarro hired Defendant for the position of road supervisor. As a road supervisor, Defendant was responsible for checking on and assisting the security officers that were stationed at each of Navarro's customers. On January 8, 2013, Defendant's supervisor, Glenn Topping, demoted him from road captain to an officer. Defendant did not return to work after that date, and Navarro officially terminated Defendant's employment on January 18, 2013.

[1] The following facts are taken from the trial, viewed in the light most favorable to the Government. *See United States v. Wright*, 392 F.3d 1269, 1273 (11th Cir. 2004). Because Defendant challenges the sufficiency of the evidence as to only one of his convictions, the facts focus on those relevant to the conviction at issue, as well as the sentencing challenges Defendant raises on appeal.

On January 27, 2013, Vern Reynolds, Navarro's technical manager and system administrator, was alerted to an issue concerning Navarro's server. While he was investigating the issue, Reynolds discovered that 12 years' worth of files were missing from the server. Reynolds was the only one with authorization to delete files from the server and he had not done so. Although he was able to recreate most of the files, he was unable to recreate three or four years' worth of documents.

The following day, January 28, 2013, the printer at Navarro stopped functioning and ultimately needed a new motherboard and operating system. In addition, the Navarro website was directing users to the websites of Navarro's competitors. That same day, Reynolds received an email from Topping regarding Topping's departure from Navarro. The email stood out to Reynolds because he knew that Topping was not in the office that day. Indeed, Topping had been let go for budgetary reasons a few days earlier. When Reynolds discovered that Topping's computer was turned on and running, he concluded that it was being controlled by someone else from a remote location.

Reynolds's subsequent review of Topping's hard drive revealed that a software program called LogMeIn—a program that allows a person to connect remotely to another computer—had been installed on Topping's computer in December 2012. Another program called Cain & Abel—which captures the

username and password of anyone logging into a computer—was also installed on the computer. Reynolds ultimately learned that Topping's computer had been remotely connected to on January 26, 27, and 28, from an IP address that was registered to Defendant's home address. Reynolds was the only person authorized to install a program such as LogMeIn onto one of Navarro's computers and he had not done so.

Approximately two weeks later, on February 18, 2013, Navarro's human resources director, Linda Blades, received a confirmation email from B&H Photo regarding a purchase order totaling $3,349.79. The purchase order was made by Maryam Ayam and paid for using a credit card in Ayam's name. However, the order was to be shipped to 6928 Southwest 39th Street, Apt. 206, Fort Lauderdale, FL, 33314. Blades recognized the shipping address as the one Defendant had provided to Navarro as his home address. Blades had not made the purchase and she confirmed that Ayam was not a Navarro employee. B&H Photo later canceled the order after Ayam confirmed it was fraudulent. The bank statement for Ayam's credit card showed that she had purchased Destiny Patrol Software in February 2013. The statement also showed that Ayam received a new credit card number during the March 2013 billing cycle.

In addition, Blades received email confirmations for two other orders made in February 2013: one for an interactive pen display totaling $2,499 and the other

for an Apple iPad in the amount of $1,188.70. Both orders were made under the name John Flores, were paid for with John Flores's credit card, and listed Flores's employer at the time, Platt Security, as the billing address. The shipping address listed on the purchase orders, however, was Defendant's address. Neither Flores nor Blades made either of these purchases. Like Ayam, Flores had a monthly service charge to Destiny Patrol Software.

On February 25, 2013, a purchase in the amount of $1,100.98 was made to Lecor Technologies using Mark Silverberg's credit card. The order was placed from a computer at the Equus gatehouse—a location where Navarro has an employee stationed to work. A subsequent investigation revealed that the Equus computer had been logged into from a LogMeIn account at an IP address registered to Defendant's home address. Silverberg did not place the order, but like Ayam and Flores, he had a transaction with Destiny Patrol Software between January and February 2013.

In May 2013, law enforcement officials executed a search warrant at Defendant's apartment. A forensic analysis of one of the computers seized from the apartment revealed programs used to access emails and login-emails for different people associated with destinypatrolsoftware.com. Officials also determined that the same computer had not only accessed Destiny Patrol Software's administrative website—which had billing and credit card

information—but that Defendant was logged in as a superuser, meaning that he had more advanced privileges than a typical user. The computer contained LogMeIn files, as well as a file that contained Topping's biographical information, including his address, date of birth, social security number, and employment information.

B. Procedural History

In 2016, a federal grand jury issued an indictment charging Defendant with: (1) intentionally causing damage without authorization to a protected computer, in violation of 18 U.S.C. § 1030(a)(5)(A) and (c)(4)(B)(i) (Count 1); (2) knowingly using one or more unauthorized access devices with intent to defraud, in violation of 18 U.S.C. § 1029(a)(2) (Count 2); and (3) three counts of aggravated identity theft, in violation of 18 U.S.C. § 1028A(a)(1) (Counts 3–5). Count 4 charged that Defendant knowingly used the means of identification of "M.A.," or Maryam Ayam. Defendant pled not guilty and proceeded to trial.

At trial, the Government presented testimony from various witnesses, including representatives from Navarro, law enforcement officials, and two of the people whose credit cards were used fraudulently, Flores and Silverberg. Ayam did not testify at trial. At the close of the Government's case-in-chief, Defendant moved for judgment of acquittal. Of relevance to this appeal, he argued that as to Count 4, the evidence was insufficient to show that any use of Ayam's credit card

was not authorized because she had not testified at trial. The court denied his motion.

Defendant testified in his own defense. He denied having hacked into Navarro's computer system and stated that he did not know about the hacking until the Federal Bureau of Investigation executed the search warrant at his apartment. He denied destroying Navarro's files and sending emails from Topping's account. He also denied connecting remotely to Navarro's computer system in order to purchase merchandise using other people's credit card numbers. After the defense rested, Defendant renewed his motion for judgment of acquittal. The court denied the motion. The jury returned a guilty verdict as to all five counts.

In preparation for sentencing, the probation officer prepared a Presentence Investigation Report ("PSR"). The PSR assigned Defendant a base offense level of 6, pursuant to U.S.S.G. § 2B1.1(a)(2). Defendant received the following enhancements: (1) an 8-level enhancement under § 2B1.1(b)(1)(E) because the loss was more than $95,000 but less than $150,000; (2) a 2-level enhancement under § 2B1.1(b)(10)(C) for sophisticated means; (3) a 2-level enhancement under § 2B1.1(b)(17) because the defendant was convicted of an offense under 18 U.S.C. § 1030 and the offense involved the intent to obtain personal information or the public dissemination of personal information; and (4) a 4-level enhancement under § 2B1.1(b)(18)(A)(ii) because he was convicted of an offense under

§ 1030(a)(5)(A). Defendant also received a two-level upward adjustment under U.S.S.G. § 3B1.3 because he used a special skill in a manner that facilitated concealment of the offense. Finally, he received a two-level enhancement for obstruction of justice under § 3C1.1. Defendant's total offense level was 26.

Based on a criminal history category of I and a total offense level of 26, Defendant's guideline range was 63 to 78 months' imprisonment. The PSR also stated that Counts 3, 4, and 5 carried a mandatory two-year term of imprisonment that must run consecutive to any other term of imprisonment. Of relevance to this appeal, Defendant objected to the two-level enhancement under § 2B1.1(b)(17). He argued that the offense he was convicted of under § 1030—intentionally causing damage to a protected computer without authorization—did not involve an intent to obtain personal information or the public dissemination of personal information. Defendant also objected to the two-level enhancement for obstruction of justice under § 3C1.1.

At the sentencing hearing, the Government asserted that the § 2B1.1(b)(17) enhancement should apply because Defendant was convicted of an offense under § 1030 and the relevant conduct for that offense demonstrated an intent to obtain personal information. Specifically, Defendant hacked into Navarro's server and accessed Blades's and Topping's personal email accounts. Additionally, Defendant viewed payroll information before deleting files from the Navarro

server. Defendant responded that the enhancement should only apply where the § 1030 offense contains as an element the intent to obtain personal information. Because Defendant's offense of conviction—§ 1030(a)(5)(A)—contained no such element, he argued that the enhancement should not apply. The district court overruled Defendant's objection, concluding that he was convicted of an offense under § 1030 and that the Government had established by a preponderance of the evidence that the relevant conduct related to his conviction demonstrated an intent to obtain personal information.

As to Defendant's objection to the enhancement for obstruction of justice, the Government argued that the enhancement should apply because Defendant testified falsely regarding a material matter during trial. Defendant responded that the enhancement was unconstitutional because it punishes defendants for exercising their right to testify where they ultimately do not prevail at trial. The district court overruled the objection. The district court sustained another objection not relevant to this appeal, resulting in an amended guideline range of 51 to 63 months' imprisonment as to Counts 1 and 2, followed by the consecutive 24-month sentence as to Counts 3 through 5.

Defendant requested a downward variance, emphasizing his age, lack of criminal history, and computer-related talent. The Government asserted that a guideline sentence was reasonable given the seriousness and sophistication of the

offenses, Defendant's interest in exerting power and control over the world, and his overall lack of honesty and candor. After considering the parties' statements, the PSR, and the 18 U.S.C. § 3553(a) factors, the court sentenced Defendant to 84 months' imprisonment. The sentence consisted of a 60-month sentence as to Counts 1 and 2, to run concurrently, a 24-month sentence as to Counts 3 to run consecutive to Counts 1 and 2, and a 24-month sentence as to Counts 4 and 5, to run concurrently with each other and to the sentence in Count 3. This appeal followed.

II. DISCUSSION

A. Sufficiency of the Evidence

Defendant argues that the evidence was insufficient to convict him of Count 4—aggravated identity theft under 18 U.S.C. § 1028A(a)(1).[2] Count 4 charged Defendant with using the means of identification of another person, specifically the debit card of Mayam Ayam, without lawful authority. Defendant asserts that the Government failed to prove beyond a reasonable doubt that Ayam's identification was used without authorization because she did not testify at trial.

We review *de novo* whether the evidence was sufficient to sustain a criminal conviction. *United States v. Jiminez*, 564 F.3d 1280, 1284 (11th Cir. 2009). In

[2] Defendant does not challenge the sufficiency of the evidence as to any of his other convictions and has therefore abandoned any challenge he may have had. *See United States v. Jernigan*, 341 F.3d 1273, 1283 n.8 (11th Cir. 2003) (providing that issues that are not raised plainly and prominently in an appellate brief are deemed abandoned).

reviewing the denial of a motion for judgment of acquittal, we view the evidence in the light most favorable of the jury's verdict. *Id.* The evidence will be sufficient to sustain a conviction if a reasonable trier of fact could find that it established the defendant's guilt beyond a reasonable doubt. *Id.* at 1284–85. When the Government relies on circumstantial evidence, the conviction must be supported by reasonable inferences, not mere speculation. *United States v. Friske*, 640 F.3d 1288, 1291 (11th Cir. 2011).

To establish a conviction under 18 U.S.C. § 1028A, "the evidence must establish that the defendant: (1) knowingly transferred, possessed, or used; (2) the means of identification of another person; (3) without lawful authority; (4) during and in relation to a felony enumerated in § 1028A(c)." *United States v. Barrington*, 648 F.3d 1178, 1192 (11th Cir. 2011) (quotations omitted); 18 U.S.C. § 1028A. Defendant argues only that the Government failed to establish that he acted without lawful authority when he used Ayam's credit card. Because he does not challenge the sufficiency of the evidence as to any of the other § 1028A elements, he has abandoned any such challenge he may have had. *See Jernigan*, 341 F.3d at 1283 n.8.

Here, the evidence presented at trial was sufficient to support Defendant's conviction for aggravated identity theft in Count 4. Although Ayam did not testify, the Government presented circumstantial evidence at trial from which a reasonable

jury could infer that Ayam did not authorize Defendant to use her credit card. Indeed, the Government presented evidence showing that the purchase order made in Ayam's name and paid for using Ayam's credit card listed the shipping address as Defendant's address. Moreover, the confirmation email for the order was not sent to Ayam. Instead, it was sent to Blades's email address at Navarro and Ayam was not a Navarro employee. Further, Ayam's bank statements show that she received a new card number in March 2013, which was the billing cycle immediately following the purchase order made on February 18, 2013. Records also showed that the purchase order was canceled after Ayam reported it to be fraudulent.

The evidence further showed that the three identity-theft victims—Ayam, Flores, and Silverberg—all had transactions with Destiny Patrol Software. Law enforcement officials discovered that Defendant's computer had login email addresses from different people associated with destinypatrolsoftware.com. Both Flores and Silverberg testified that the purchases made in their names were not authorized, and, like Ayam, these purchase orders listed Defendant's home address as the location where the items were to be shipped. Given the similarities between the three purchase orders, a reasonable jury could infer that Ayam's card was used without lawful authority.

Finally, Defendant took the stand in his own defense and denied having engaged in any misconduct, including having used other people's credit cards. Because the jury returned a guilty verdict, it obviously did not believe Defendant's statements and we may consider this as substantive evidence of guilt. *See United States v. Kendrick*, 682 F.3d 974, 985 (11th Cir. 2012) ("[W]hen a criminal defendant chooses to testify on his own behalf, his statements, if disbelieved by the jury, may be considered as substantive evidence of his guilt."). Based on this evidence, a reasonable jury could conclude that Defendant acted without Ayam's authorization when he used her credit card. Accordingly, the evidence was sufficient to support Defendant's conviction on Count 4.

B. Defendant's Sentence

Using a two-step process, we review the reasonableness of a district court's sentence for an abuse of discretion. *United States v. Cubero*, 754 F.3d 888, 892 (11th Cir. 2014). We first look to whether the district court committed any significant procedural error, such as miscalculating the advisory guideline range, treating the Sentencing Guidelines as mandatory, failing to consider the 18 U.S.C. § 3553(a) factors,[3] selecting a sentence based on clearly erroneous facts, or failing

[3] The § 3553(a) factors include: (1) the nature and circumstances of the offense and the history and characteristics of the defendant; (2) the need to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for the offense; (3) the need for deterrence; (4) the need to protect the public; (5) the need to provide the defendant with needed education or vocational training or medical care; (6) the kinds of sentences available; (7) the Sentencing Guidelines range; (8) pertinent policy statements of the Sentencing Commission;

to adequately explain the chosen sentence. *Id.* Then we examine whether the sentence is substantively reasonable in light of the totality of the circumstances. *Id.* The party challenging the sentence bears the burden of showing that it is unreasonable. *United States v. Pugh*, 515 F.3d 1179, 1189 (11th Cir. 2008).

A. Procedural Reasonableness

1. U.S.S.G. § 2B1.1(b)(17) Enhancement

Defendant challenges the district court's application of a two-level enhancement under § 2B1.1(b)(17). We review a district court's factual findings for clear error and its interpretation of the Sentencing Guidelines *de novo*. *United States v. Perez*, 366 F.3d 1178, 1181 (11th Cir. 2004).

Section 2B1.1(b)(17) of the Sentencing Guidelines provides for a two-level increase in a defendant's offense level if "the defendant was convicted of an offense under 18 U.S.C. § 1030, and the offense involved an intent to obtain personal information, or . . . the offense involved the unauthorized public dissemination of personal information." U.S.S.G. § 2B1.1(b)(17). Defendant argues that the district court erred by applying the enhancement under § 2B1.1(b)(17) because 18 U.S.C. § 1030(a)(5)(A)[4]—the statute of conviction—

---

(9) the need to avoid unwarranted sentencing disparities; and (10) the need to provide restitution to victims. 18 U.S.C. § 3553(a).

[4] Section 1030(a)(5)(A) provides that a defendant violates the statute if he "knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct,

does not involve "an intent to obtain personal information" or "the unauthorized public dissemination of personal information." Stated another way, Defendant asserts that the § 2B1.1(b)(17) enhancement applies only where the § 1030 offense in question includes as an element "an intent to obtain personal information" or "the unauthorized public dissemination of personal information."

We are not, however, persuaded by Defendant's narrow interpretation of the term "offense" under § 2B1.1(b)(17). The term "offense" is broadly defined in the Guidelines to mean "the offense of conviction and all relevant conduct under § 1B1.3 (Relevant Conduct) unless a different meaning is specified or is otherwise clear from the context." U.S.S.G. § 1B1.1, comment. (n.1(H)) (emphasis added); *see United States v. De La Cruz Suarez*, 601 F.3d 1202, 1221 (11th Cir. 2010) (explaining that the term offense is defined as "the offense of conviction" and "all relevant conduct"). Relevant conduct, in turn, is defined as "all acts and omissions committed, aided, abetted, counseled, commanded, induced, procured, or willfully caused by the defendant . . . that occurred during the commission of the offense of conviction." U.S.S.G. § 1B1.3(a)(1)(A). Section 2B1.1(b)(17) does not specify a different meaning for the term offense, nor is it clear from the context that the term

---

intentionally causes damage without authorization, to a protected computer." 18 U.S.C. § 1030(a)(5)(A).

should be interpreted differently under this provision. *See* U.S.S.G. § 1B1.1, comment. (n.1(H)); U.S.S.G. § 2B1.1(b)(17).

To support his argument, Defendant asserts that because there are certain subsections of § 1030 that require an intent to obtain personal information or the public dissemination of information, the § 2B1.1(b)(17) enhancement should apply to convictions under those subsections, not to his offense of conviction, § 1030(a)(5)(A). One of the subsections Defendant identifies is § 1030(a)(2)(C), which makes it a violation for a defendant to "intentionally access[] a computer without authorization or exceed[] authorized access, and thereby obtain[] . . . information from any protected computer." 18 U.S.C. § 1030(a)(2)(C). Contrary to Defendant's assertions, however, § 1030(a)(2)(C) does not contain an element of intent to obtain personal information or involve the public dissemination of personal information. *See* 18 U.S.C. § 1030(a)(2)(C). We are therefore not persuaded by this argument.

Here, the district court determined that the enhancement under § 2B1.1(b)(17) applied because Defendant was convicted of an offense under § 1030, namely § 1030(a)(5)(A), and the relevant conduct related to that offense involved the intent to obtain personal information. We discern no error in the district court's interpretation of this enhancement. Moreover, Defendant does not challenge the district court's finding that the relevant conduct related to the offense

involved the intent to obtain personal information.[5] Accordingly, the district court did not err by applying the two-level enhancement under § 2B1.1(b)(17).[6]

2. Obstruction-of-Justice Enhancement

Defendant also challenges the district court's imposition of a two-level enhancement for obstruction of justice under U.S.S.G. § 3C1.1. Specifically, he argues that the district court failed to make an explicit finding that he willfully obstructed justice. Defendant, however, did not challenge the enhancement on this basis before the district court. Instead, he argued that the enhancement unfairly punished him for exercising his constitutional right to testify. Because Defendant argues for the first time on appeal that the district court was required to make an explicit willfulness finding, our review is limited to plain error.[7] *See United States*

[5] But regardless, the district court did not clearly err by finding that the conduct related to the offense involved the intent to obtain personal information. Specifically, Defendant hacked into Navarro's computer system by using programs that enabled him to capture usernames and passwords. In doing so, he gained access to, among other things, payroll information and Topping's email account and other biographical information. *See* U.S.S.G. § 2B1.1, comment. (n.1) (defining "personal information" to mean "sensitive or private information involving an identifiable individual" including private correspondence, such as emails, medical records, or financial records).

[6] The Government also argues that the district court's application of the enhancement under § 2B1.1(b)(17) does not constitute double counting. Because this argument was not "plainly and prominently" raised in Defendant's brief, we do not address this argument. *See Jernigan*, 341 F.3d at 1283 n.8.

[7] "The plain-error test has four prongs: there must be (1) an error (2) that is plain and (3) that has affected the defendant's substantial rights; and if the first three prongs are met, then a court may exercise its discretion to correct the error if (4) the error 'seriously affects the fairness, integrity or public reputation of judicial proceedings.'" *United States v. Madden*, 733 F.3d 1314, 1320 (11th Cir. 2013) (alteration accepted) (quoting *United States v. Olano*, 507 U.S. 725, 732 (1993).

v. Rodriguez, 398 F.3d 1291, 1298 (11th Cir. 2005) (providing that a sentencing objection raised for the first time on appeal is reviewed for plain error).

We conclude that the district court did not err, plainly or otherwise, by applying the obstruction-of-justice enhancement without making an explicit finding that Defendant willfully provided false testimony. Section 3C1.1 of the Guidelines provides for a two-level increase in a defendant's offense level if "the defendant willfully obstructed or impeded, or attempted to obstruct or impede, the administration of justice with respect to the investigation, prosecution, or sentencing of the instant offense of conviction, and . . . the obstructive conduct related to (A) the defendant's offense of conviction and any relevant conduct; or (B) a closely related offense." U.S.S.G. § 3C1.1.

The Guidelines' commentary identifies perjury as an example of conduct that warrants application of the enhancement. U.S.S.G. § 3C1.1, comment. (n.4(B)). For purposes of this enhancement, the Supreme Court has defined perjury as "false testimony concerning a material matter with the willful intent to provide false testimony, rather than as a result of confusion, mistake, or faulty memory." *United States v. Dunnigan*, 507 U.S. 87, 94 (1993). Although the district court should make specific factual findings concerning the elements of perjury, we have explained that application of the obstruction-of-justice enhancement may be affirmed where the district court makes a general finding that

the defendant committed perjury as to material matters and that finding is supported by the record. *United States v. Dobbs*, 11 F.3d 152, 155 (11th Cir. 1994); *see also United States v. Hatney*, 80 F.3d 458, 463 (11th Cir. 1996) ("[W]e may affirm a district court's enhancement even absent particularized findings regarding the defendant's perjury so long as the district court found in general that the defendant's testimony was perjurious as to material matters and the record supports that finding.").

In the present case, the district court concluded that Defendant "provided materially false testimony under oath in that he specifically denied his involvement in intruding into the Navarro computer testimony" and therefore "is being punished for providing perjured testimony." Although the district court did not make an explicit finding as to willfulness, the record amply supports the district court's finding that Defendant perjured himself on material matters when he unequivocally denied any involvement in the intrusion into Navarro's computer system. Indeed, the evidence showed that Defendant installed programs on Navarro's computers that enabled him to access usernames and passwords and to connect remotely to Navarro's computer system. Additionally, the forensic analysis of Defendant's computer showed that he had accessed Topping's email account, his biographical information, and Navarro's payroll information. Moreover, during his testimony, Defendant did not indicate that he was confused or mistaken about his recollection

of the issues in this case. *See Dunnigan*, 507 U.S. at 95 (indicating that inaccurate testimony does not constitute perjury if it is the result of confusion, mistake, or a faulty memory). In short, Defendant cannot establish that the district court's application of the obstruction-of-justice enhancement constituted plain error.

B. Substantive Reasonableness

Finally, Defendant argues that his sentence is substantively unreasonable. We disagree. First, Defendant's 84-month sentence—which consisted of a 60-month sentence as to Counts 1 and 2 and a consecutive 24-month sentence as to Counts 3, 4, and 5—was within the guideline range of 51 to 63 months' imprisonment as to Counts 1 and 2 and the mandatory 24-month sentence as to each of Counts 3 through 5. *See United States v. Hunt*, 526 F.3d 739, 746 (11th Cir. 2008) (explaining that this Court normally expects a sentence within the guideline range to be reasonable). The 60-month sentence as to Counts 1 and 2 was also significantly below the statutory maximum of 120 months' imprisonment for those offenses. *See United States v. Gonzalez*, 550 F.3d 1319, 1324 (11th Cir. 2008) (explaining that a sentence well below the statutory maximum is an indicator of reasonableness). And notably, the district court had discretion to run the 24-month sentences as to Counts 3 through 5 consecutive to each other, but instead chose to run them concurrent to each other. *See* 18 U.S.C. § 1028A(b)(2), (b)(4).

Defendant's 84-month sentence is also supported by the § 3553(a) factors, including the nature and circumstances of the offense and Defendant's history and characteristics. As noted by the district court, Defendant's offenses were serious and complex. Indeed, the Government emphasized that Defendant's crimes—which involved hacking into his former employer's computer system, accessing email accounts and other personal information of employees, destroying files, and obtaining credit card numbers to make unauthorized purchases—were not isolated or spur-of-the-moment offenses, but instead had required deliberate planning and preparation over a period of time.

Although Defendant argues that the court did not adequately consider his lack of criminal history or the fact that his actions were merely an immature response to his demotion at Navarro, the weight the court assigned to each factor was entirely within its discretion. *See United States v. Rosales-Bruno*, 789 F.3d 1249, 1254 (11th Cir. 2015) ("The decision about how much weight to assign a particular sentencing factor is 'committed to the sound discretion of the district court.'" (quoting *United States v. Williams*, 526 F.3d 1312, 1322 (11th Cir. 2008)). And contrary to Defendant's argument that the district court sentenced him based on its assumption that he harbored anti-government sentiments, the district court explicitly stated that it was giving Defendant the benefit of the doubt that he was not an anti-government supporter.

In short, we are not "left with the definite and firm conviction that the district court committed a clear error of judgment in weighing the § 3553(a) factors by arriving at a sentence that lies outside the range of reasonable sentences dictated by the facts of the case." *United States v. Irey*, 612 F.3d 1160, 1190 (11th Cir. 2010) (quotations omitted). Accordingly, Defendant has not met his burden of showing that his 84-month sentence is substantively unreasonable.

III. CONCLUSION

Based on the foregoing reasons, Defendant's convictions and sentences are **AFFIRMED.**