UNPUBLISHED

UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

No. 13-4567

UNITED STATES OF AMERICA,

Plaintiff – Appellee,

v.

ROBERT EDWIN STEELE,

Defendant – Appellant.

Appeal from the United States District Court for the Eastern District of Virginia, at Alexandria. Gerald Bruce Lee, District Judge. (1:12-cr-00515-GBL-1)

Argued: September 19, 2014 Decided: December 24, 2014

Before DIAZ and THACKER, Circuit Judges, and Paul W. GRIMM, United States District Judge for the District of Maryland, sitting by designation.

Affirmed by unpublished opinion. Judge Diaz wrote the opinion, in which Judge Thacker and Judge Grimm joined.

ARGUED: Jonathan P. Sheldon, SHELDON, FLOOD & HAYWOOD, PLC, Fairfax, Virginia, for Appellant. Alexander T.H. Nguyen, OFFICE OF THE UNITED STATES ATTORNEY, Alexandria, Virginia, for Appellee. **ON BRIEF:** Dana J. Boente, Acting United States Attorney, OFFICE OF THE UNITED STATES ATTORNEY, Alexandria, Virginia, for Appellee.

DIAZ, Circuit Judge:

Petitioner Robert Steele spent nine months secretly logging in to the email server of his former employer, gaining access to confidential and proprietary information related to its government contract bids. As a result, Steele was convicted for crimes under the Computer Fraud and Abuse Act. Steele now appeals his conviction, as well as his sentence of imprisonment and restitution. We reject Steele's contentions of error and consequently affirm the judgment of the district court.

I.

In 2007, Platinum Solutions, Inc., hired Steele as its vice president for business development and backup systems administrator. His duties gave him access to the company's server, which allowed him to monitor email accounts and employee passwords. Three years after Steele joined Platinum, the company was sold to SRA International, Inc. Steele subsequently resigned and went to work for another company, which--like Platinum and SRA--provided contract IT services to government defense agencies. During the next nine months, Steele continued to log in to SRA's server via a "backdoor" account he had used while working for Platinum and SRA, and he proceeded to access and download documents and emails related to SRA's ongoing

contract bids. The FBI later determined that Steele had accessed the server almost 80,000 times.

A grand jury indicted Steele on two counts of wire fraud under 18 U.S.C. §§ 1343 and 1349, and fourteen counts of unauthorized access of a protected computer under the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030.[1] The district court granted a judgment of acquittal on the wire fraud charges pursuant to Rule 29 of the Federal Rules of Criminal Procedure, but a jury convicted Steele on all of the CFAA charges, consisting of two misdemeanor and twelve felony counts. Steele received a prison sentence totaling 48 months, significantly less than the recommendations under the U.S. Sentencing Guidelines Manual ("U.S.S.G."). In addition, the district court ordered him to pay $50,000 in fines, $1,200 in fees, and $335,977.68 in restitution.

II.

Steele presents four major arguments on appeal. He first contends that the evidence was insufficient to convict him of accessing a protected computer "without authorization." He further contends that his conviction should be reversed because

[1] A "protected computer" includes one "used in or affecting interstate or foreign commerce." § 1030(e)(2).

the district court's jury instructions constructively amended the indictment by referring to the separate crime of accessing a computer in "excess of authorization." Moreover, he asserts that the enhancement of his charges to felonies under 18 U.S.C. § 1030(c)(2)(B)(ii) violated his due process rights and the constitutional prohibition against double jeopardy. Finally, Steele challenges his prison sentence and the order to pay restitution based on the district court's failure to properly apply the U.S.S.G. and restitution statute. We address each argument in turn.

A.

Steele first contends that the evidence is insufficient to support his convictions for accessing a protected computer "without authorization" under the CFAA. In considering this claim, we view the evidence in the light most favorable to the government, and we must affirm the convictions if there "is evidence that a reasonable finder of fact could accept as adequate and sufficient to support a conclusion of a defendant's guilt beyond a reasonable doubt." United States v. Pasquantino, 336 F.3d 321, 332 (4th Cir. 2003) (en banc) (quoting United States v. Burgos, 94 F.3d 849, 862 (4th Cir. 1996) (en banc)). Because it was reasonable for the jury to conclude that Steele acted "without authorization" when accessing SRA's computer server, we affirm Steele's convictions.

The CFAA imposes criminal and civil penalties on individuals who unlawfully access computers. Specifically, § 1030(a)(2)(C), under which Steele was indicted, prohibits accessing a protected computer "without authorization" or in "exce[ss of] authorized access." Notably, the indictment itself charged Steele with violating only the first prong of this section.

Steele primarily relies on our opinion in WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199 (4th Cir. 2012), to argue that because SRA did not change his access password when he resigned, Steele's post-employment access, though "ethically dubious" was not "without authorization" as contemplated by the statute. We cannot agree.

WEC Carolina contributes to a dialogue among the circuit courts on the reach of § 1030(a)(2). The broad view holds that when employees access computer information with the intent to harm their employer, their authorization to access that information terminates, and they are therefore acting "without authorization" under § 1030(a)(2). See Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 420–21 (7th Cir. 2006). The narrower construction, adopted by WEC Carolina, holds that § 1030(a)(2) applies to employees who unlawfully access a protected computer, but not to the improper use of information lawfully accessed. See WEC Carolina, 687 F.3d at 203-04 (citing

United States v. Nosal, 676 F.3d 854, 863 (9th Cir. 2012) (en banc)).

Importantly, this split focuses on employees who are authorized to access their employer's computers but use the information they retrieve for an improper purpose. Steele's case is distinguishable for one obvious reason: he was not an employee of SRA at the time the indictment alleges he improperly accessed the company's server. In WEC Carolina, authorization did not hinge on employment status because that issue was not in dispute. Here, by contrast, the fact that Steele no longer worked for SRA when he accessed its server logically suggests that the authorization he enjoyed during his employment no longer existed. See, e.g., LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1136 (9th Cir. 2009) ("There is no dispute that if Brekka accessed LVRC's information . . . after he left the company . . . , Brekka would have accessed a protected computer 'without authorization' for purposes of the CFAA."); Restatement (Third) of Agency § 3.09 (2006) (Actual authority terminates "upon the occurrence of circumstances on the basis of which the agent should reasonably conclude" that authority is revoked.).

Common sense aside, the evidence provides ample support for the jury's verdict. SRA took steps to revoke Steele's access to company information, including collecting Steele's company-issued laptop, denying him physical access to the company's

offices, and generally terminating his main system access. And Steele himself recognized that his resignation effectively terminated any authority he had to access SRA's server, promising in his resignation letter that he would not attempt to access the system thereafter. Just because SRA neglected to change a password on Steele's backdoor account does not mean SRA intended for Steele to have continued access to its information.

Because Steele clearly acted "without authorization" under the plain meaning of § 1030(a)(2), the evidence is sufficient to affirm his convictions.

B.

The government charged Steele with "intentionally accessing a computer without authorization." The indictment did not, however, purport to charge Steele under the alternative crime in § 1030(a)(2): exceeding authorized access. Nevertheless, when instructing the jury, the district court twice stated that Steele had been charged with "intentionally accessing a computer without authorization and in excess of authorization . . . ." J.A. 781–83 (emphasis added). Steele urges that these erroneous instructions constituted a constructive amendment of the indictment requiring reversal. We disagree.

A constructive amendment (or fatal variance) occurs when the court "broadens the possible bases for conviction beyond those presented by the grand jury." United States v. Foster,

507 F.3d 233, 242 (4th Cir. 2007) (quoting United States v. Floresca, 38 F.3d 706, 710 (4th Cir. 1994) (en banc)). It is distinguishable from a non-fatal variance, which occurs when the facts proven at trial differ in some nonessential way from the facts alleged in the indictment, or when the court fails to instruct the jury on an essential element of the charged offense. See Floresca, 38 F.3d at 709–10.

We review de novo the question of whether the district court constructively amended the indictment. United States v. Allmendinger, 706 F.3d 330, 339 (4th Cir. 2013). Under this circuit's precedent, the finding of a constructive amendment requires reversal, even where--as here--a defendant fails to preserve the error. See Floresca, 38 F.3d at 714.

Steele contends that the district court's references to the "exceeds authorization" language of § 1030(a)(2) amount to a constructive amendment because they provide an additional, unindicted basis for the jury to convict him. While it may be true that instructing the jury on the elements of an "exceeds authorization" charge or explicitly changing the indictment to reflect this charge could constitute a constructive amendment, the district court's two references to "exceeding authorization" do not rise to this level.

Indeed, our cases hold that a variance or misstatement is not fatal if the indictment, evidence, and jury instructions as

a whole support conviction on the crime charged. See, e.g., United States v. Lentz, 524 F.3d 501, 514 (4th Cir. 2008) (finding that the "indictment, evidence, instructions, and arguments . . . viewed in their totality" made "implausible" the claim that the court's supplemental instruction amounted to a constructive amendment); United States v. Velez, 27 F. App'x 179, 181 (4th Cir. 2001) (per curiam) (concluding that because the court made clear that the defendant was "not on trial for any act . . . not alleged in the indictment" and "sent a copy of the indictment and a verdict form to the jury room," a misstatement by the court while reading the instructions did not amount to a constructive amendment).

In this case, the district court's references to "in excess of authorization" occurred in the context of the court's instructions regarding the statutory felony enhancements:

> Counts 3 through 16 charge Mr. Robert Edwin Steele with intentionally accessing a computer without authorization and in excess of authorization and that the value of the information obtained exceeded $5,000.
>
> . . .
>
> Counts 3 through 16 charge[] the defendant, Mr. Robert Edwin Steele, with intentionally accessing a computer without authorization and in excess of authorization and that the offense was committed in furtherance of a criminal and tortious act in violation of . . . the laws of the Commonwealth of Virginia . . . .

J.A. 781–83 (emphasis added). The court thereafter instructed the jury on how it should calculate the value of the information obtained and on the elements of the Virginia grand larceny statute that supported the felony enhancements. Nowhere did the court, as Steele contends, expressly tell the jury that it could find Steele guilty if it found he had acted "in excess of his authorization."

We note that the parties took pains to ensure that the district court's written instructions did not contain the "exceeds authorization" language, and the court expressly struck that language from the instructions. The court also read the indictment to the jury, without the "exceeds authorization" language. In addition, the court's recitation of the elements included only the charge of accessing a computer "without authorization." Moreover, the court told the jury that it was to consider the instructions "as a whole" in reaching its decision and that Steele was not on trial for any act not charged in the indictment. Finally, the jury received a copy of the indictment and the verdict forms based on the indictment.

Given that the bulk of the district court's instructions to the jury correctly referred to the charge as accessing a computer "without authorization," we conclude that the court's two isolated references to accessing a computer "in excess" of authorization did not constitute a constructive amendment.

C.

Next, Steele asserts that his felony convictions under § 1030(c)(2)(B)(iii) are constitutionally flawed. Typically, accessing a protected computer without authorization is a misdemeanor offense under the CFAA. The statute does, however, provide three ways through which the offense may be enhanced to a felony: (1) committing the offense for "commercial advantage or private financial gain"; (2) committing the offense "in furtherance of any criminal or tortious act in violation of" state or federal law; or (3) if "the value of the information obtained exceeds $5,000." 18 U.S.C. § 1030(c)(2)(B) (2012). Accordingly, the indictment charged Steele not only with accessing a protected computer without authorization but also with doing so on the basis of these three felony enhancements, including in furtherance of Virginia's grand larceny statute, Va. Code Ann. section 18.2-95.

Steele first argues that the Virginia statute and the CFAA provision are proved using the same criminal conduct. According to Steele, because the two offenses merge, the government was barred by double jeopardy principles from enhancing what would have been a misdemeanor into a felony conviction. Second, Steele argues that he could not be convicted of grand larceny under the Virginia statute because "intangibles" such as computer data cannot be the subject of common law larceny under

Virginia law. Consequently, enhancing his offenses to felonies on this basis violates his due process rights.

Because Steele did not preserve these objections to his convictions, we review them for plain error. See United States v. Hastings, 134 F.3d 235, 239 (4th Cir. 1998) (citing United States v. Olano, 507 U.S. 725, 731–32 (1993)). As we explain, no error, plain or otherwise, occurred. Steele's arguments cannot upend common sense conclusions that the Virginia statute does not present a merger problem, nor that Steele could be convicted under the statute.

1.

Steele relies heavily on our decision in United States v. Cioni, 649 F.3d 276 (4th Cir. 2011), to support his double jeopardy argument. That case involved the defendant's unlawful accessing of email accounts and her subsequent viewing of emails contained in those accounts. Id. at 279–81. Cioni was consequently convicted of accessing a computer without authorization (in violation of § 1030(a)(2)(C)), and her conviction was enhanced to a felony on the theory that her conduct was "in furtherance of" obtaining unauthorized access to communications in electronic storage (a violation of 18 U.S.C. § 2701(a)). Id. at 281.

Cioni challenged her convictions by arguing that the government used the same conduct--her unlawful accessing and

viewing of email accounts--to support both the underlying violation of § 1030(a)(2)(C) and the felony enhancement under § 2701(a). Id. We agreed, holding that such an "overlap" creates a "merger problem, tantamount to double jeopardy." Id. at 282–83 (quoting United States v. Santos, 553 U.S. 507, 527 (2008) (Stevens, J., concurring in the judgment) (internal quotation marks omitted)).

Steele likewise contends that his conduct of accessing protected computers improperly supported both a violation of § 1030(a)(2)(C) and the accompanying felony enhancement under Va. Code Ann. section 18.2-95. We disagree. Primarily, proof of § 1030(a)(2)(C) requires only that the defendant read or observe data; "[a]ctual asportation . . . need not be proved . . . ." See United States v. Batti, 631 F.3d 371, 377 (6th Cir. 2011) (quoting S. Rep. No. 99-432, 6–7 (1986), reprinted in 1986 U.S.C.C.A.N. 2479, 2484). The Virginia statute, on the other hand, criminalizes grand larceny, which by definition requires proof of an actual taking. See Dunlavey v. Commonwealth, 35 S.E.2d 763, 764 (Va. 1945); Welch v. Commonwealth, 425 S.E.2d 101, 104 (Va. Ct. App. 1992).

In this case, Special Agent Etienne, who investigated Steele's conduct, testified that the FBI recovered evidence that Steele not only accessed emails and bid documents but actively downloaded them and saved them to multiple hard drives connected

to his personal computer. J.A. 700–02 (describing Steele's organized and purposeful method for saving documents in labeled file folders on his hard drive). In addition, the government provided the jury with a summary chart of the charges against Steele, listing specific documents supporting those charges, the value associated with those documents, and the location where they were found on Steele's computer hard drives. J.A. 1069.[2] Through this evidence, the government was able to show that Steele's conduct included not simply reading or observing protected information but also downloading ("taking") that information.

In sum, because the government used different conduct to prove the two offenses, Steele's felony convictions for

[2] The documents listed under Counts 7, 8, 11, 12, and 13 of the summary chart have no corresponding hard drive location, presumably because the government could not establish that Steele actually downloaded those documents. However, the district court instructed the jury that it could also find Steele guilty of a felony if (1) he accessed the computer data for "commercial advantage or private financial gain" or (2) "the value of the information obtained exceed[ed] $5,000." The jury considered substantial evidence that both additional felony enhancements existed. J.A. 551–55 (testimony of Agent Etienne describing Steele's access and downloads of documents related to bids for which his new company competed with his old); J.A. 993–1018 (charts showing development costs of the information accessed by Steele); J.A. 1069 (summary chart estimating proprietary value of the information accessed and downloaded by Steele). This evidence fully supported the jury's felony verdicts on Counts 7, 8, 11, 12, and 13.

violating the CFAA do not raise the double jeopardy concerns implicated by Cioni.

2.

Steele similarly relies on Carter v. Commonwealth, 682 S.E.2d 77 (Va. Ct. App. 2009), to contend that his felony convictions under the CFAA violate his due process rights. In Carter, the defendant was convicted of stealing paint from a retail store. On appeal, he argued that the evidence was insufficient to convict him of larceny because he never intended to keep the paint, but rather sought to return it for a cash refund. 682 S.E.2d at 79–81. The court rejected Carter's argument, but it also rejected the government's separate contention that the value of the paint could be subject to larceny, noting that "an intangible cannot be the subject of larceny." Id. at 81 & n.7 (internal quotation marks omitted). Steele argues that, likewise, computer data--as an intangible--is not subject to larceny, and therefore he could not be convicted under the Virginia statute.

We reject this contention. Virginia law expressly provides that,

> For the purposes of § 18.2-95 . . ., personal property subject to . . . larceny . . . shall include:
>
> 1. Computers and computer networks;

> 2. Financial instruments, computer data, computer programs, computer software and all other personal property regardless of whether they are:
>
> a. Tangible or intangible . . . .

Va. Code Ann. § 18.2-152.8 (West 2011) (emphasis added). Under this section, intangible computer data may be subject to larceny, even common law larceny, as codified by section 18.2-95. Moreover, we find Carter distinguishable. Not only is theft of an amorphous concept like value more properly considered an intangible than computer data (which is only "intangible" in that it is electronic), there is also no Virginia statute that expressly includes "value" in the type of property subject to larceny. Accordingly, we conclude that Steele could have been convicted under the Virginia grand larceny statute for accessing and downloading the proprietary information of his former employer.

D.

Lastly, we reject Steele's contentions that the government erred in calculating both his sentence under the U.S.S.G. and the amount of restitution required under the Mandatory Victims Restitution Act of 1996 ("MVRA"), 18 U.S.C. § 3663A. We review both sentencing and restitution judgments under a deferential abuse of discretion standard. Gall v. United States, 552 U.S.

38, 41 (2007); United States v. Harvey, 532 F.3d 326, 339 (4th Cir. 2008).

The district court accepted the recommendation of the presentence investigation report that Steele's base offense level be increased by 18 points under U.S.S.G. § 2B1.1(b)(1) because his theft caused more than $2,500,000 in loss. The court arrived at the loss estimate ($3,048,769.55) by looking at the costs incurred by SRA to prepare the documents accessed by Steele relating to specific government contracts for which his new company competed with his old. Steele argues that, in increasing his offense level to account for intended loss, the government failed to show that Steele had the subjective intent to cause the amount of loss calculated.

Our precedent is clear that when calculating loss under § 2B1.1(b)(1), intended loss (rather than actual loss) is the appropriate measure. See United States v. Miller, 316 F.3d 495, 499 (4th Cir. 2003). Although Steele testified that he did not have the subjective intent to cause his former employer any loss, the district court did not accept his explanation. J.A. 1101 (Steele's explanation was "farfetched."); J.A. 1118 ("Well, I just don't buy it."); J.A. 1120 ("[Y]ou say, 'I just had [this information] on my computer. I did nothing with it.' I don't buy that either."). Because the court accounted for Steele's subjective intent when determining his sentence, its conclusion

was not in error. See United States v. Cloud, 680 F.3d 396, 409 n.7 (4th Cir. 2012) (finding that the court's rejection of the defendant's argument that there was no intended loss "adequately accounted for [his] subjective intent").

We are also satisfied that the district court imposed a reasonable amount in restitution. Under the MVRA, a court must award restitution where the defendant is convicted of an offense against property and the victim suffers pecuniary loss. 18 U.S.C. § 3663A(c)(1) (2012). Restitution must include both the victim's "expenses incurred during participation in the investigation or prosecution of the offense" and the value of any stolen property (if return of the property "is impossible, impracticable, or inadequate"). § 3663A(b)(1)(B), (b)(4).

The district court awarded $228,400 in restitution for the amount spent by SRA to assist in the investigation and prosecution of the offenses. Further, the court awarded $91,462.80, as a fractional component of the development costs of the stolen proprietary information. Finally, the court awarded $16,114.88 in legal fees, for a total restitution award of $335,977.68.

Steele contests the district court's restitution order on two grounds: first, that no evidence supported the $228,400 amount, and second, that the court erred in its calculation of SRA's actual loss. We disagree on both counts.

First, the district court concluded that the $228,400 amount was reasonable given that 11 SRA employees spent over 1,083 hours assisting the authorities in investigating and prosecuting the offenses. Although this number differs from the $75,330 that the government proffered at trial for the time spent by those same 11 employees, the increase is understandable in light of the additional time required to testify and help prepare for the trial.

Second, the $91,462.80 actual loss amount reflects the district court's decision to award SRA only 3% of its estimated cost of preparing the bid documents that Steele accessed. The MVRA requires restitution to be based on the victim's total actual loss. See Harvey, 532 F.3d at 339. While it is unclear why the district court chose to award SRA only a fraction of its total loss, any error in the court's calculation inured in Steele's favor. Accordingly, we decline to disturb the district court's restitution award.

III.

For the reasons given, we affirm the district court's judgment.

AFFIRMED