[DO NOT PUBLISH]

IN THE UNITED STATES COURT OF APPEALS

FOR THE ELEVENTH CIRCUIT

No. 15-11276
Non-Argument Calendar

D.C. Docket No. 1:14-cr-20641-KMW-1

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

versus

REGINALD STEELE NELSON,

Defendant-Appellant.

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

(February 16, 2018)

Before WILSON, WILLIAM PRYOR, and MARTIN, Circuit Judges.

PER CURIAM:

Reginald Steele Nelson appeals his below-guidelines sentence of 96 months of imprisonment following his pleas of guilty to six crimes connected to his use of

stolen identification information to file fraudulent claims for federal disability benefits, unemployment benefits, tax refunds, and food assistance benefits. The district court enhanced Nelson's base offense level by 16 levels based on an actual loss of $236,371.45 and an intended loss of $895,000 attributable to his possession of social security numbers and dates of birth of about 1,790 persons. *See* United States Sentencing Guidelines Manual § 2B1.1(b)(1)(I) & cmt. n.3(F) (Nov. 2014). Nelson argues that none of the 1,790 compromised identifiers qualify as "access devices," *see* 18 U.S.C. § 1029(e)(1), and he also argues, for the first time, that his sentence is procedurally unreasonable because the district court impermissibly considered his refusal to cooperate. We conclude, based on our recent ruling in *United States v. Wright*, 862 F.3d 1265, 1275 (11th 2017), "that a social security number qualifies as an 'access device'" and that Nelson was subject to an enhancement for a loss amount of $500 for each compromised social security number. But we cannot say that the district court made a reasonable estimate of the amount of loss because it failed to identify the number of compromised social security numbers and to address whether the dates of birth qualified as access devices. We also conclude that the district court did not consider Nelson's alleged failure to cooperate in selecting his sentence. We vacate Nelson's sentence and remand for the district court to determine how many of the compromised

identifiers count as access devices, to compute the amount of loss, and to resentence Nelson.

I. BACKGROUND

Nelson pleaded guilty to one count of using with intent to defraud one or more debit cards to obtain $1,000 or more, 18 U.S.C. § 1029(a)(2) (Count 1); one count of using 15 or more stolen social security numbers, *id.* § 1029(a)(3) (Count 2); one count of possessing a credit card skimming device, *id.* § 1029(a)(4) (Count 3); and three counts of aggravated identity theft, *id.* § 1028A(a)(1) (Counts 4-6). The Department of Labor detected the fraud after discovering that numerous unemployment compensation claims had been submitted electronically from Nelson's internet protocol address. Nelson had accessed unemployment compensation websites thousands of times and used the names, dates of birth, and other identifying information of real persons to file 90 fraudulent claims with the State of Florida and 9 fraudulent claims with the State of New York. Investigators obtained video surveillance recordings and still photographs that showed Nelson withdrawing cash from automatic teller machines using credit and debit cards containing unemployment benefits.

When investigators arrested Nelson, he had in his pocket a list of "approximately 40 distinct pieces of [personal identification information]." Inside Nelson's residence, investigators discovered 85 debit and credit cards that were

embossed with the names of real persons or were encoded with direct deposit numbers that accessed government benefits. Investigators also discovered "at least 1,800 distinct pieces of [personal identification information], including handwritten names, social security numbers, dates of birth, addresses, phone numbers, 'secret questions' and answers, insurance policy numbers, and tax returns" recorded "in notebooks and printouts from officers, schools, and hospitals" along with "handwritten notes giving additional information about" the viability of the stolen information. Investigators determined that Nelson had defrauded a "total of 1,920 individuals"; he had caused "approximately 48 . . . individuals [to be] . . . temporarily deprived of their actual SSA benefits"; and he had exploited the identities of at least 473 real persons.

Nelson's presentence investigation report held him responsible for an actual loss of $236,371.45, which was attributable to the 130 persons whose benefits he had downloaded to 85 debit and credit cards, and an intended loss of $895,000, which represented one access device for each of the remaining 1,790 victims multiplied by $500, *see* U.S.S.G. § 2B1.1 cmt. n.3(F). Nelson's report grouped Counts 1-3 and assigned him a total offense level of 28, which included a 16-level enhancement for a loss amount of $1,131,371.45, *id.* § 2B1.1(b)(1)(I). Based on Nelson's criminal history of I, the presentence report provided an advisory

guideline range of 78 to 97 months for Counts 1-3 and a sentence of 24 months for each of his three convictions for aggravated identity theft.

Nelson objected to the intended loss of $895,000 on the ground it overrepresented the number of access devices, and in the alternative, he requested a downward variance to reflect the "actual loss" he caused of $236,371.45. Nelson conceded that he "was in possession of dates of birth and social security numbers of approximately 1,790 persons," but he argued that those identifiers constituted "means of identification" instead of "access devices." He also argued that the 85 debit and credit cards were the only items that qualified as access devices, which would reduce his enhancement from 16 levels to 12 levels, *id.* § 2B1.1(b)(1)(G), and result in a total offense level of 24. The government responded that Nelson's use of social security numbers, names, and dates of birth to obtain money qualified as unauthorized access devices and that each of the 1,790 compromised identifiers should be multiplied by $500 to calculate his intended loss amount.

At the request of the district court, the parties filed supplemental sentencing memoranda addressing whether to use $500 or $100 as the multiplier to compute Nelson's loss amount. The government argued that the guidelines and caselaw supported assessing $500 per access device, and Nelson agreed. But Nelson replied that he was entitled to a downward variance.

The district court overruled Nelson's objection to the amount of loss and, based on the parties' agreement that the guidelines supported an assessment of $500 for each access device, it adopted the loss amount and advisory sentencing range provided in the presentence report. The district court stated that $500 multiplier "actually might be too small a number" given the effects of identity theft, and it considered the seriousness of Nelson's crimes and "the importance of deterrence" because Nelson had reoffended after evading prosecution in 2009 for access device fraud. "Taking all that into account," the district court granted "a modest [downward] variance" because Nelson was "pursuing his education [at a community college], he [had] a [drug rehabilitation] sponsor[,]" and "he [had] been by all accounts a good father." The district court "attributed a $100 value" to each of the 1,790 compromised identifiers, which reduced Nelson's enhancement from 16 to 14 levels and resulted in a sentencing range of 63 to 78 months. The district court sentenced Nelson to three concurrent terms of 72 months for Counts 1-3 and to 24 months for each of his three aggravated identity theft offenses, with those 24-month terms running concurrently with each other but consecutively to his 72-month sentence.

II. STANDARDS OF REVIEW

We review *de novo* the interpretation of the Sentencing Guidelines. *United States v. Dabbs*, 134 F.3d 1071, 1079 (11th Cir. 1998). "[T]he determination of

monetary loss [is reviewed] under the clearly erroneous standard." *Id.* at 1081. When a defendant fails to object at sentencing to the consideration of an impermissible factor, we review for plain error. *United States v. Vandergrift*, 754 F.3d 1303, 1309 (11th Cir.2014).

III. DISCUSSION

We divide our discussion in two parts. First, we address the calculation of Nelson's loss amount. Second, we address whether the district court considered Nelson's lack of cooperation when imposing his sentence.

A. The District Court Must Make Further Findings of Fact About the Amount of Loss.

Nelson argues that the 1,790 compromised identifiers were incorrectly classified as access devices, which resulted in the enhancement of his sentence based on an inflated amount of loss. The government responds that all the stolen identifiers qualified as access devices. Due to the failure of the parties and the district court to address whether dates of birth qualify as access devices or to quantify the amount of loss attributable to the two categories of identifiers, we must vacate Nelson's sentence and remand for resentencing.

We affirm the determination that the social security numbers Nelson possessed qualify as access devices. We held recently in *Wright* "that a social security number qualifies as an 'access device' under the definition in 18 U.S.C. § 1029(e)(1)." 862 F.3d at 1275. *Wright* forecloses Nelson's challenge to the

enhancement of his sentence for a loss amount attributable to compromised social security numbers. Nelson admitted that he possessed authentic social security numbers that qualified as access devices.

Although the social security numbers that Nelson possessed qualify as access devices, we cannot say whether the district court made a reasonable estimate of the amount of loss. "[A] court need only make a reasonable estimate of the loss, given the available information," *id.* at 1276 (quoting *United States v. Moran*, 778 F.3d 942, 973 (11th Cir. 2015)), "[h]owever, there must be at least some evidence on which to base a reasonable estimate of how many [identifiers] fell within the definition of an 'access device,'" *id.* Nelson argues that he possessed "1,790 pieces of [personal identification information]," and in his sentencing memorandum, he identified the compromised identifiers as "dates of birth and social security numbers." Nelson faces an enhancement for a loss of $500 for each compromised social security number, *id.* at 1275–76, but the record contains no evidence of how many social security numbers he possessed. Neither the presentence investigation report, the parties, nor the district court quantified the social security numbers or dates of birth or quantified the loss attributable to each of those two categories of identifiers. When Nelson and the government focused their dispute on whether social security numbers qualified as access devices, the district court failed to differentiate between the compromised identifiers or to

address whether the dates of birth qualified as access devices. The district court must determine whether the dates of birth qualify as access devices and how many access devices Nelson possessed. "Accordingly, we must remand this case to the district court to address again, and make fact findings about, the loss amount." *Id.* at 1276.

The issue whether dates of birth can qualify as access devices is one of first impression in our circuit, but our precedent provides the district court some guidance. As we observed in *Wright*, access devices include objects and identification information that can be used in connection with an access device to obtain anything of value or that can be used to initiate a transfer of funds. *Id.* at 1274.

Congress defined "access device" as follows:

> the term "access device" means any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument).

18 U.S.C. § 1029(e)(1). Congress used "broader statutory language in an effort to anticipate future criminal activities and thereby provide greater protection to all participants in the payment device system, including those that honor payment devices and consumers." *Dabbs*, 134 F.3d at 1081 (quoting S. Rep. No. 98-368, at

5, reprinted in 1984 U.S.C.C.A.N. 3647, 3651) (ellipses and brackets omitted). That policy has led us to "broadly construe the statutory language of section 1029 to include the innovative means that parties use to gain unauthorized information to engage in fraudulent activities." *Id.* We have concluded that section 1029(e)(1) prohibits the fraudulent use of usernames and passwords, *United States v. Barrington*, 648 F.3d 1178, 1202 (11th Cir. 2011), routing and bank account numbers, *United States v. Williams*, 790 F.3d 1240, 1250 (11th Cir. 2015), merchant account numbers, *Dabbs*, 134 F.3d at 1080–81, and social security numbers, *Wright*, 862 F.3d at 1275.

On remand, the district court must determine Nelson's loss amount and his appropriate sentencing range under the Sentencing Guidelines. The amount of "loss is the greater of actual loss or intended loss." U.S.S.G. § 2B1.1 cmt. n.3(A). "Intended loss (I) means the pecuniary harm that the defendant purposely sought to inflict; and (II) includes intended pecuniary harm that would have been impossible or unlikely to occur." *Id.* § 2B1.1 cmt. n.3(A)(ii). And a special rule that applies to access devices instructs that the "loss includes any unauthorized charges made with the counterfeit . . . or unauthorized access device and shall be not less than $500 per access device." *Id.* § 2B1.1 cmt. n.3(F)(i). The district court must determine how many social security numbers Nelson possessed and the amount of loss attributable to those access devices. The district court also must determine whether

the dates of birth Nelson possessed qualify as access devices. Because the parties neglected to make any substantive arguments about the classification of the compromised dates of birth or the quantity of the two categories of identifiers, they may submit additional evidence on those issues. *See Wright*, 862 F.3d at 1276.

B. The District Court Did Not Consider Nelson's Failure to Cooperate.

Nelson argues that the district court plainly erred by basing his sentence on his failure to cooperate with the government, but the district court did not consider Nelson's lack of cooperation as a factor in selecting his sentence. The district court took into account the seriousness and effects of Nelson's crimes and the need to deter him from committing similar future crimes, and then decided to vary downward and impose a sentence below Nelson's advisory guideline range based on his personal circumstances. *See* 18 U.S.C. § 3553(a).

IV. CONCLUSION

We **VACATE** Nelson's sentence and **REMAND** for resentencing.