

UNITED STATES COURT OF APPEALS FOR THE FIRST CIRCUIT

United States v. Rueda

United States v. Rueda, 933 F.3d 6 (1st Cir. 2019) · No. No. 18-1962 · Decided July 31, 2019

SUMMARY

The First Circuit held that under U.S.S.G. §2B1.1, Application Note 3(F)(i), a \$500 minimum loss per access device applies to each counterfeit or unauthorized credit card number, regardless of whether the number was actually used or could be shown to successfully obtain value. The court rejected the defendant's arguments that the government must prove each number "can be used" under 18 U.S.C. §1029(e)(1) or that the \$500 minimum only applies to devices actually charged. The court affirmed the district court's loss calculation of \$1,290,000 (2,580 numbers × \$500) based on numbers linked to financial institutions and found with skimming equipment, even though actual losses were only \$24,673.60, and upheld the variant sentence of four months' imprisonment.

OPINION

BARRON, J.

United States Court of Appeals For the First Circuit No. 18-1962 UNITED STATES, Appellee, v. MEYLISI RUEDA, Defendant, Appellant. APPEAL FROM THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF MAINE [Hon. Nancy Torresen, U.S. District Judge] Before Howard, Chief Judge, Thompson and Barron, Circuit Judges. J. Hillary Billings, Assistant Federal Defender was on brief for appellant.

Renee M. Bunker, Assistant United States Attorney, Appellate Chief, with whom Halsey B. Frank, United States Attorney, was on brief, for appellee. July 31, 2019 BARRON, Circuit Judge. Meylisi Rueda ("Rueda") pleaded guilty to one count of conspiracy to commit access-device fraud, in violation of 18 U.S.C. § 1029(a)(2), (a)(3), and (b)(2), in the District Court for the District of Maine.

She now challenges the District Court's sentence resulting from that plea. She argues that the District Court erred in its calculation of the "loss" attributable to her offense, due to what, she argues, was an incorrect reading of § 2B1.1(b)(1) of the United States Sentencing Guidelines.

We affirm. I. Beginning in June of 2016, state and federal law enforcement agencies initiated an investigation into multiple complaints of credit card fraud originating in Maine. Law enforcement agents received information in connection with that investigation that Yaisder Herrera Gargallo, Jose Castillo Febles, Juan Carlos Febles, and Rueda, had, over the span of several months, used

fraudulent credit cards to purchase merchandise, gift cards, airline tickets, and to lease rental vehicles.

On June 18, 2016, law enforcement agents stopped a Jeep in Brunswick, Maine that matched the description of a vehicle used during the fraudulent credit card transactions under investigation. Rueda was not in the vehicle when it was pulled over, but Gargallo, Jose Castillo Febles, and Juan Carlos Febles were.

The agents questioned the three passengers, who admitted in - 2 - response that they, along with Rueda, were participants in a fraudulent credit card scheme; that they had traveled from Florida to Maine to undertake that scheme; and that they had stolen credit cards in their possession at the time that they were pulled over. A search of the vehicle led agents to discover multiple packages of unopened merchandise (e.g., a Dewalt drill set and three iPads), multiple credit cards bearing stolen account information, credit card "skimming" equipment, and a laptop.

A forensic search of the laptop revealed nine text files that contained what appeared to be credit card information. Agents identified what they determined were numbers for 2,732 unique credit cards in these files. In addition to the text files, the forensic search of the laptop revealed various programs associated with the manufacture of fake credit cards.

Investigators were able to identify the issuing financial institutions associated with 2,580 of the 2,732 apparent credit card numbers that were retrieved from the laptop's text files. Most of these financial institutions did not submit victim impact statements. Eight of them did.

The victim impact statements that those eight financial institutions submitted averred that the losses associated with the card numbers from the laptop text files that were associated with their institutions totaled, collectively, \$24,673.60. - 3 - On October 6, 2017, Rueda pleaded guilty to one count of conspiracy to commit access-device fraud, in violation of 18 U.S.C. § 1029(a)(2), (a)(3), and (b)(2).

The District Court then requested a pre-sentence report ("PSR"), which the United States Office of Probation prepared and disclosed on November 24, 2017. The PSR recommended, pursuant to the Guidelines, a guidelines sentencing range ("GSR") of 37-46 months of imprisonment.

The PSR based the GSR on the Guidelines' "loss" definition. Section 2B1.1 of the guidelines defines "loss" as "the greater of actual loss or intended loss." § 2B1.1, cmt. n.3(A). "Actual loss" is defined as "the reasonably foreseeable pecuniary harm that resulted from the offense." *Id.* at cmt. n.3(A)(i). "Intended loss," by contrast, is defined as "the pecuniary harm that the defendant purposely sought to inflict [which] includes intended pecuniary harm that would have been impossible or unlikely to occur."

Id. at cmt. n.3(A)(ii). The Guidelines provide additional instructions for calculating "loss" in cases that involve "Stolen or Counterfeit Credit Cards and Access Devices." Id. at cmt. n.3(F)(i) [hereinafter Application Note 3(F)(i)]. These instructions provide that, "[i]n a case involving any counterfeit access device or unauthorized access device, loss includes any unauthorized charges made with the counterfeit access device or unauthorized access device and shall be not less than \$500 per access device." - 4 - Section 2B1.1 further states that "counterfeit access device" and "unauthorized access device" are defined in accordance with 18 U.S.C. § 1029(e).

Id. at cmt. n.10(A). Section 1029(e) of the United States Criminal Code defines "access device" as "any card, plate, code, account number, electronic serial number, mobile identification number, [or] personal identification number... that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value."

18 U.S.C. § 1029(e)(1). That section of the federal criminal code defines "counterfeit access device" as "any access device that is counterfeit, fictitious, altered, or forged, or an identifiable component of an access device or a counterfeit access device." Id. at § 1029(e)(2).

Finally, that section of the federal criminal code defines "unauthorized access device" as "any access device that is lost, stolen, expired, revoked, canceled, or obtained with intent to defraud." Id. at § 1029(e)(3).

After applying the Application Note 3(F)(i), the PSR determined that the "loss" totaled \$1,290,000. The PSR did so by attributing a loss of \$500 to each of the 2,580 numbers retrieved from the laptop text files that had been determined to constitute unauthorized or counterfeit access devices. Rueda objected to the PSR's loss calculation. She contended that to apply Application Note 3(F)(i)'s \$500 minimum - 5 - loss amount to each of the 2,580 credit card numbers at issue, the government would first need to establish that each "can be used... to obtain money, goods, services, or any other thing of value," in accordance with the statutory definition of an access device.

See 18 U.S.C. § 1029(e)(1). Rueda further contended that there was no evidentiary basis for the government to make such a showing. Accordingly, she contended that the "loss" that could be attributed to her offense was no more than the \$24,673.60 of loss that the eight financial institutions had described in their victim impact statements. At sentencing, on October 1, 2018, the District Court noted that the question of the loss calculation was "close" but ultimately rejected Rueda's contention.

The District Court adopted, instead, the GSR of 37-46 months of imprisonment based on the PSR's attribution of a loss of \$500 to each of the 2,580 numbers retrieved from the laptop's text files determined to be counterfeit or unauthorized access devices.

The District Court did note, however, that the difference between the GSR based on the PSR's "loss" calculation and the GSR based on Rueda's proposed calculation was "profound." Thus, given various mitigating factors that the District Court identified, it imposed a variant sentence of four-months imprisonment followed by two years of supervised release. Additionally, the District Court ordered a joint and several restitution obligation of \$24,673.60 on Rueda - 6 - and her co-defendants.

Finally, the District Court granted a motion to stay Rueda's sentence, pending appeal, to allow Rueda the opportunity to receive an answer from our Court on the "loss issue." Rueda timely appealed her sentence. Our review is de novo, as her challenge to her sentence turns on a matter of guidelines interpretation. *United States v. Flores-Machicote*, 706 F.3d 16, 19 (1st Cir.

2013). II. Rueda first contends that the District Court erred in applying Application Note 3(F)(i)'s \$500 minimum loss amount to each of the 2,580 credit card numbers in making its loss calculation under the Guidelines, because the government failed to establish that, in accord with 18 U.S.C. 1029(e)(1)'s definition of an "access device," each of those numbers "can be used... to obtain money, goods, services, or any other thing of value."

18 U.S.C. § 1029(e)(3). But, we do not agree. Application Note 3(F)(i) incorporates the definition of "counterfeit" and "unauthorized" access devices in 18 U.S.C. § 1029(e)(2) and 18 U.S.C. § 1029(e)(3), respectively.

Thus, Application Note 3(F)(i) necessarily requires that a \$500 minimum loss be attributed to each access device of that type, see *United States v. Moon*, 808 F.3d 1085, 1092 (6th Cir. 2015) (concluding that Application Note 3(F)(i)'s express use of the terms - 7 - "counterfeit" and "unauthorized" access devices indicated that any usability requirement must be permissive enough to encompass such devices in its scope), save for possibly available exceptions not relevant here, see Application Note 3(F)(i) (describing the exception for "telecommunication" access devices).

As a result, by the plain terms of Application Note 3(F)(i), the \$500 minimum loss amount must be attributed even to, for example, a "fictitious" "expired, revoked, [or] canceled" access device. 18 U.S.C. § 1029(e)(2)-(3).

As a result, we do not see how Rueda's contention that Application Note 3(F)(i) must be read to exclude from its scope the 2,580 numbers that are at issue here is a tenable one. Rueda does contend that Application Note 3(F)(i) incorporates the "can be used" requirements from the definition of an "access device" in § 1029(e)(3). She does not develop, however, any argument that would explain why, given this record, these 2,580 numbers do not qualify as the kind of "unauthorized" or "counterfeit" access devices to which Application Note 3(F)(i) plainly applies.

To be sure, Rueda argues that nothing about Application Note 3(F)(i)'s express inclusion of "unauthorized" and "counterfeit" access devices precludes the conclusion that it contains an

implicit usability requirement. According to her, even "expired, revoked, or canceled" access devices can be "used" in limited ways, such as by "manually impress[ing] [the fraudulent - 8 - cards] onto a paper receipt" and "present[ing] [the fraudulent cards] over the phone... when electronic access is temporarily unavailable."

But, if this is the definition of "can be used" that Rueda contends should apply here, then we fail to see on what basis she means to contend that it would not encompass every one of the 2,580 numbers at issue here. Rueda cannot supportably argue that any of those 2,580 numbers is just a random string of sixteen digits that happened to be stored on the co-conspirators' computer.

Each of the 2,580 credit card numbers was linked, by a bank identification number, to an identifiable financial institution. Each of those 2,580 credit card numbers was also discovered along with physical credit cards bearing stolen credit card information, software used to manufacture fake credit cards, products purchased using stolen credit cards, and "skimming" equipment used to steal credit card information from gas station customers.

Rueda does rely on the out-of-circuit case *United States v. Onyesoh*, 647 F.3d 1157 (9th Cir. 2012), in which the Ninth Circuit did clearly endorse a usability requirement. But, we do not read that precedent to hold that the government must show that a credit card number could successfully obtain money before such a number could be subject to the \$500 minimum "loss" amount for "counterfeit" and "unauthorized" access devices pursuant to Application Note 3(F)(i).

Thus, even that precedent does not - 9 - support her challenge on this score, given this record. See *id.* at 1160 (holding that evidence of expired cards "in combination with another device" such as an "embosser" would potentially suffice to establish usability). III. Rueda separately contends that Application Note 3(F)(i)'s use of the phrase "shall not be less than \$500 per access device" merely modifies "loss includes any unauthorized charges made with the counterfeit access device or unauthorized access device."

(Emphasis added). Accordingly, Rueda contends, the "most logical and reasonable" reading of Application Note 3(F)(i) is that its \$500 minimum loss amount may be attributed to an access device only when it was actually "charge[d]" during the commission of the offense. And, so read, Rueda contends, Application Note 3(F)(i) would not permit the \$500 loss amount to be attributable to any of the 2,580 numbers at issue here, given that the government has not shown that any of them were actually charged.

As a result, Rueda argues that the loss attributable to her offense should not be the \$1,290,000 calculated by the District Court. It should be the \$24,673.60 that was reflected in the victim impact statement that the eight financial institutions submitted. But, here too, we disagree.

The word "loss" in Application Note 3(F)(i) operates as the subject for the two verb clauses that follow and that are connected by a conjunction: - 10 - "includes any unauthorized charges made

with the counterfeit access device or unauthorized access device" and "shall be not less than \$500 per access device."

Accordingly, the sentence is most naturally read so that these two verb clauses have the same subject: "loss." So read, Application Note 3(F)(i) provides that "loss" both (1) shall "include[] any unauthorized charges made with the counterfeit access device or unauthorized access device" and (2) "shall be not less than \$500 per access device" regardless of whether each access device was actually charged.

This reading accords -- as Rueda's reading does not -- with Section 2B1.1(b)(1)'s broader instruction that "loss" include "intended loss," which is defined as "intended pecuniary harm that would have been impossible or unlikely to occur." *Id.* at cmt. n.3(A)(ii) (emphasis added). This reading also comports with the rest of Application Note 3(F)(i)'s language, which appears to establish a special carve-out from the \$500 limit for only a certain type of unauthorized access device -- a telecommunications access device -- that is merely possessed and not used. § 2B1.1, cmt. n.3(F)(i).

That carve-out indicates that -- contrary to Rueda's contention -- the higher \$500 minimum loss amount generally does apply to unauthorized or counterfeit access devices that a defendant merely possesses and has not otherwise used. See *United States v. Cardenas*, 598 F. App'x 264, 267 (5th Cir. 2015) (concluding that the language in the telecommunications provision - 11 - indicates that the loss calculation in the previous sentence encompassed both used and unused devices); *United States v. Thomas*, 841 F.3d 760, 764 (8th Cir.

2016) (concluding the same). Finally, this reading accords with the reading given to Application Note 3(F)(i) by every circuit to have addressed the argument about its scope that Rueda now advances. See, e.g., *Cardenas*, 598 F. App'x at 267 (concluding that "nothing in the text [of Application Note 3(F)(i)] requires the access devices to be actually used" (emphasis in original)); *Thomas*, 841 F.3d at 764 ("[Application Note 3(F)(i)] does not require that the device actually have been used."); *United States v. Gilmore*, 431 F. App'x 428, 430-31 (6th Cir.

2011) ("The plain language [of Application Note 3(F)(i)] sets a floor for calculating the loss attributable to each device, namely \$500; it does not limit loss calculations to devices actually used."). IV. The District Court here noted the "profound" disparity between the "loss" as calculated by Rueda's PSR and the actual "loss" attributed to her offense based on the victim impact statements submitted by the various financial institutions.

But, the District Court, based on that disparity and various mitigating factors, exercised its discretion to impose a variant sentence of four-months imprisonment followed by two years of supervised release. We thus conclude that the District Court did not err in - 12 - imposing the sentence that it did. *United States v. Popovski*, 872 F.3d 552, 554 (7th Cir.

2017) ("If a calculation under Application Note 3(F)(i) overstates the seriousness of the offense, a district judge must adjust accordingly."). Accordingly, we affirm the District Court's sentence. - 13

-