

**FOR PUBLICATION**  
**UNITED STATES COURT OF APPEALS**  
**FOR THE NINTH CIRCUIT**

UNITED STATES OF AMERICA, <i>Plaintiff-Appellee,</i> v. LESLIE N. ONYESOH, an individual, <i>Defendant-Appellant.</i>
---

No. 10-50480  
D.C. No.  
2:09-CR-00565-DSF  
OPINION

Appeal from the United States District Court  
for the Central District of California  
Dale S. Fischer, District Judge, Presiding

Argued and Submitted  
January 13, 2012—Pasadena, California

Filed April 4, 2012

Before: William A. Fletcher and Raymond C. Fisher,  
Circuit Judges, and Jack Zouhary, District Judge.\*

Opinion by Judge Zouhary

---

\*The Honorable Jack Zouhary, District Judge for the U.S. District Court for the Northern District of Ohio, Toledo, sitting by designation.

---

**COUNSEL**

Hassan Gorguinpour (argued), Law Office of Hassan Gorguinpour, Cerritos, California, and Mark Yanis, Huntington Beach, California, for the defendant-appellant.

Amanda Miller Bettinelli (argued) and Curtis Arthur Kin, Office of the U.S. Attorney, Los Angeles, California, for the plaintiff-appellee.

---

**OPINION**

ZOUHARY, District Judge:

**INTRODUCTION**

This appeal addresses access device fraud under 18 U.S.C. § 1029 and, specifically, whether the Government must prove

the usability of an expired credit card number in order for a district court to enhance a sentence. We find evidence of usability is required and vacate the sentence because the Government failed to carry its burden.

### BACKGROUND

In May 2009, postal agents conducted a search of Defendant-Appellant Leslie Onyesoh's ("Defendant") home resulting in the discovery of, among other things, stolen mail, credit cards, and a spreadsheet containing 500 expired credit card numbers. Defendant pled guilty to possession of stolen mail and access device fraud, including the knowing possession of "fifteen or more . . . unauthorized access devices" with the intent to defraud. 18 U.S.C. § 1029 (a)(3). An unauthorized access device is defined as "any access device that is lost, stolen, expired, revoked, canceled, or obtained with intent to defraud." § 1029(e)(3). Under the statute's definition of "access device," the device must be capable of obtaining "money, goods, services, or any other thing of value." § 1029(e)(1).

The presentence report concluded that the 500 expired credit card numbers were unauthorized access devices and recommended a 12-level enhancement under U.S. Sentencing Guidelines § 2B1.1(b)(1)(G) for a loss greater than \$200,000. The report arrived at this dollar figure because Application Note 3(F)(i) assesses a minimum loss of \$500 per device. As explained in the report:

[Defendant] possessed credit cards belonging to at least 14 different account holders (\$7,000), 19 credit card profiles, including credit card account numbers (\$9,500), a typed spread sheet containing victim profiles and credit card account numbers of approximately 500 different individuals (\$250,000), and one check for \$1,096.57. Onyesoh also caused an actual loss of \$43,098.92 to three victims. Considering

these figures, the total loss is approximately \$310,695.49. Accordingly, a 12-level increase applies.

The enhancement was the focus of the sentencing hearing, where Defendant objected to the loss calculation. Defendant conceded that expired credit cards could be unauthorized access devices, but only if their usability was also shown. The Government countered that such proof was not required and, in any event, there was “no doubt” expired credit card numbers *could* provide a credit history or help establish a new credit account. The district court applied the enhancement, accepting the Government’s argument that the expired credit card numbers were unauthorized access devices without requiring further proof of usability.

The additional loss calculated from the 500 expired credit card numbers increased the Guidelines range from 18-24 months to 37-46 months. Defendant was sentenced to 46 months. This appeal followed.

#### **JURISDICTION AND STANDARD OF REVIEW**

The district court had jurisdiction under 18 U.S.C. § 3231. We have jurisdiction pursuant to 28 U.S.C. § 1291. The district court’s interpretation of the criminal statute is reviewed *de novo*. See *United States v. Carranza*, 289 F.3d 634, 642 (9th Cir. 2002). The district court’s factual findings are reviewed for clear error. *United States v. Garro*, 517 F.3d 1163, 1167 (9th Cir. 2008). “[A] material error in calculating the sentencing range is grounds for resentencing.” *Id.*

#### **DISCUSSION**

##### **Usability Requirement**

[1] Our analysis begins with the language of the statute. An “unauthorized access device” must be an “access device,”

which itself must be capable of obtaining “money, goods, services, or any other thing of value.” 18 U.S.C. §§ 1029(e)(1) and (e)(3). The statute’s language is clear and we give it full effect — unauthorized access devices are a subset of access devices, and therefore must be capable of obtaining something of value. *See TRW Inc. v. Andrews*, 534 U.S. 19, 31 (2001) (holding a cardinal principal of statutory interpretation is that “no clause, sentence, or word shall be superfluous, void, or insignificant”).

The statute is intended to target major fraud operations instead of individual use of “an expired or revoked card,” and the statute was written broadly in order to “encompass future technological changes.” *See* H.R. Rep. No. 98-894, at 19-20 (1984); *see also United States v. Dabbs*, 134 F.3d 1071, 1081 (11th Cir. 1998) (holding use of merchant account numbers was criminal even though those numbers were not specifically mentioned in the statute). But the *kind* of devices potentially covered by the statute says nothing about the quantum of proof necessary to establish usability. The legislative history simply does not address that issue.

No court, in this or any other circuit, has read usability out of the statute. In *United States v. Nguyen*, the defendant possessed 110 blank credit cards and was convicted of access device fraud. 81 F.3d 912, 914 (9th Cir. 1996). The defendant argued there was no evidence the blank cards were usable and therefore they were not access devices. *Id.* The court found the statute required the user to “be able to obtain goods or services,” *id.* at 915 (quoting *United States v. Bailey*, 41 F.3d 413, 418 (9th Cir. 1994)), and also determined the defendant was capable of using the blank cards because “[s]he possessed an embosser and credit card account numbers,” and was practicing how to use this equipment. *Id.*

On strikingly similar facts to the instant case, a district court found that expired credit card numbers were unauthorized access devices. *United States v. Jones*, 557 F. Supp. 2d

630 (E.D. Pa. 2008). In *Jones*, the defendant argued these expired numbers could not be used. Disagreeing, the district court noted “Jones’ argument that expired credit cards are not access devices runs contrary to the very text of the statute.” *Id.* at 638. The district court also held that the Government must prove that each access device “could have been used” to obtain value, the very issue we face here. *Id.*

In *United States v. Brewer*, a case heavily relied on by the Government, the court held long distance telephone service access codes were access devices even though many of the numbers were non-working. 835 F.2d 550, 554 (5th Cir. 1987). *Brewer* analyzed whether the definitions of “unauthorized,” under Subsection (e)(3), and “counterfeit,” under Subsection (e)(2), were mutually exclusive, and whether applying both terms to the same conduct was appropriate. *Id.* at 553. But nowhere does that case address usability.

[2] We hold that unauthorized access devices must be usable. This conclusion gives effect to the entire statute and is consistent with its plain language.

### **Proof of Usability**

[3] Defendant’s sentence was enhanced because the district court found the expired credit card numbers in his possession were unauthorized access devices. In order for the district court to make this finding, the Government had to prove the usability of the expired credit card numbers by a preponderance of the evidence. *See United States v. Cazares*, 121 F.3d 1241, 1248 (9th Cir. 1997) (holding a sentence enhancement was improper when the government failed to prove a fact by a preponderance).

[4] Of course, the amount of proof necessary will depend upon the access device at issue. For some types of access devices — *e.g.*, credit card and bank account numbers — usability may be self-evident. But while a working credit card

can clearly be used to obtain value, the usability of other types of access devices may not be readily apparent.

Presented at appellate oral argument with a hypothetical of credit card numbers that had expired 35 years ago and were useless, the Government conceded such numbers would not be covered under the statute. Here, Defendant's credit card numbers had been expired for some three years, yet the Government argued these numbers required no further proof of usability because the evidence was "overwhelming" Defendant used, or could have used, these numbers. We have carefully reviewed the record in this case and found no evidence of usability, let alone "overwhelming" evidence. There was no crossover between Defendant's victims and the list of expired numbers, and there was no showing Defendant ever took steps or attempted to use the expired numbers, or that Defendant possessed them before their expiration.

[5] In short, the Government needed to show some usability of these expired numbers. For example, the Government could have offered expert testimony to establish usability. *See United States v. Yellowe*, 24 F.3d 1110, 1113 (9th Cir. 1994) (finding the district court's calculation of an offense level correct when based on testimony that 90% of the devices were useable). Evidence that Defendant was prepared to use the numbers in combination with another device also could have satisfied the statutory requirements. *See Nguyen*, 81 F.3d at 914 (finding blank cards in combination with an embosser qualifies as access devices). The lack of any evidence is fatal. "It matters only that the user of the access device be able to obtain goods or services from which he would otherwise be excluded." *Bailey*, 41 F.3d at 418. We have no way of telling whether the expired credit card numbers, in this case, are unauthorized access devices under the statute.

#### CONCLUSION

For an unauthorized access device whose usability is not readily apparent, such as an expired credit card number, some

---

proof of usability is required when the defendant does not concede the fact or when the defendant challenges the enhancement. For the foregoing reasons, the sentence is vacated, and this case is remanded for further proceedings to allow the district court to hear evidence of usability.

VACATED and REMANDED.