

In the  
United States Court of Appeals  
For the Seventh Circuit

---

No. 16-4178

UNITED STATES OF AMERICA,

*Plaintiff-Appellee,*

*v.*

KARL POPOVSKI,

*Defendant-Appellant.*

---

Appeal from the United States District Court for the  
Northern District of Illinois, Eastern Division.  
No. 14 CR 131 — **Ronald A. Guzmán**, *Judge*.

---

ARGUED SEPTEMBER 19, 2017 — DECIDED SEPTEMBER 28, 2017

---

Before WOOD, *Chief Judge*, and EASTERBROOK and ROVNER,  
*Circuit Judges*.

EASTERBROOK, *Circuit Judge*. Karl Popovski pleaded guilty to wire fraud. 18 U.S.C. §1343. The criminal scheme entailed obtaining credit-card or debit-card numbers from abroad, encoding them onto blank cards, and using those cards to withdraw money from automated teller machines. Popovski, one of a large group directed by Gheorgui Martov that implemented this scheme, was responsible for more than 1,000

account numbers but planned to use 800 of them in Peru. The district judge disregarded those 800 numbers and calculated an intended loss based on actual or planned transactions in the United States. The judge concluded that the intended loss attributable to Popovski was \$131,000, which added eight offense levels under U.S.S.G. §2B1.1. The judge sentenced Popovski to 30 months' imprisonment, the middle of the Guidelines range (27 to 33 months). Popovski contends that his offense level and sentence should have been lower.

A card reprogrammed with a stolen number for use in an ATM is an "unauthorized access device" as defined in 18 U.S.C. §1029(e)(1), (3). Application Note 3(F)(i) to §2B1.1 provides: "In 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." In *United States v. Moore*, 788 F.3d 693 (7th Cir. 2015), we concluded that this includes all access devices that the defendant possessed, whether used or not. The district court calculated loss at \$500 per reprogrammed card or stolen number that was to be used within the United States.

Popovski maintains that a card or number counts under Application Note 3(F)(i) only if it produced money or was demonstrably functional. He insists that cards with canceled numbers, or those whose accounts or credit limits have been exhausted by earlier withdrawals, do not count toward the number of devices. He relies on *United States v. Onyesoh*, 674 F.3d 1157 (9th Cir. 2012), which held this, while the prosecutor relies on *United States v. Moon*, 808 F.3d 1085 (6th Cir. 2015), which disagreed with *Onyesoh*.

*Onyesoh* relied on the statutory definition of an “access device” in §1029(e)(1) as a card, number, or other identifier that can be “used” to obtain goods or money. (Application Note 3(F)(i) refers to this statute for the definition of “access device”.) The Ninth Circuit thought that “used” means “able to be used successfully”. But *Moon* relied on the fact that the definition of “unauthorized access device” in §1029(e)(3) includes “any access device that is lost, stolen, expired, revoked, canceled, or obtained with intent to defraud”. This necessarily implies that a card, number, or other identifier with a potential to obtain goods or initiate a transfer of funds remains an “access device” even if it is “expired, revoked, [or] canceled”. These two statutory paragraphs can work together only if paragraph (1) defines an “access device” according to its nature—the sort of thing that could in principle be used to get goods or funds, whether or not it would work in practice. Application Note 3(A)(ii)(II) adds that intended loss includes all loss that the defendant sought to inflict, including “intended pecuniary harm that would have been impossible or unlikely to occur”. Popovski does not deny that he intended to steal from all of the persons whose account information he possessed, and this Application Note tells us that his inability to carry out that intent does not diminish “loss.” Sensibly so, *Moon* observes, because even a device that cannot be used to siphon funds can injure the account’s owner by helping the thief create a false identity at the owner’s expense. 808 F.3d at 1092.

The Ninth Circuit’s conclusion was based on a desire to eliminate extreme situations, such as a long sentence based on a cache of credit cards that had been buried for a generation and dug up long after all of them had expired or been canceled, or the discovery in a museum of clay tablets that

the Persians used for banking. Like the panel in *Onyesoh*, we too think that a district judge should not increase a sentence just because the defendant possessed ancient pieces of plastic or lists of numbers useful only during the reign of Xerxes. But we disagree with *Onyesoh*'s view that this result should be achieved by treating the language in §1029(e)(3) as irrelevant to the meaning of "access device". Courts must read the statute to reconcile these paragraphs.

After *United States v. Booker*, 543 U.S. 220 (2005), all sentences must be reasonable in light of the criteria in 18 U.S.C. §3553(a), no matter what the Sentencing Guidelines say. If a calculation under Application Note 3(F)(i) overstates the seriousness of the offense, a district judge must adjust accordingly. That process, rather than warping the language of §1029(e), is the way to avoid the Ninth Circuit's parade of horrors. We accordingly agree with the Sixth Circuit's reading of the statute and Guideline 2B1.1.

Popovski does not contend that a significant fraction of the numbers encoded onto his blank cards was ancient or unlikely to work. The district judge therefore was entitled to rely on the rule in Application Note 3(F)(i) without requiring card-by-card proof of functionality while the scheme was in operation. The Application Note's aggregate approach takes account of the possibility that some access devices won't work, while others could produce more than \$500. Popovski does not contend that a sentence of 30 months is unreasonably high, in light of the statutory criteria, for his criminal conduct. He relies entirely on a contention that §1029(e)(1) requires card-by-card proof of functionality. As we have rejected that reading of the statute, the judgment is

AFFIRMED.