[DO NOT PUBLISH]

IN THE UNITED STATES COURT OF APPEALS

FOR THE ELEVENTH CIRCUIT

No. 19-11394
Non-Argument Calendar

D.C. Docket No. 1:18-cr-20760-CMA-1

UNITED STATES OF AMERICA,

Plaintiff–Appellee,

versus

ISAIAH MEME,

Defendant–Appellant.

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

(March 13, 2020)

Before BRANCH, LUCK, and ANDERSON, Circuit Judges.

PER CURIAM:

Isaiah Meme was convicted of access device fraud, in violation of 18 U.S.C. § 1029(a)(2); aggravated identity theft, in violation of 18 U.S.C. § 1028A(a)(1); and possession of 15 or more unauthorized access devices, in violation of 18 U.S.C. § 1029(a)(3). He appeals these convictions. On appeal, Meme argues that there was insufficient evidence to support his convictions. For the reasons that follow, we affirm Meme's convictions.

BACKGROUND

Because Meme appeals his conviction, specifically arguing that the evidence was insufficient to support a conviction, we review the evidence that was presented at trial in some detail. Isaiah Meme was indicted on September 18, 2018, in a multiple-count indictment alleging 1 count of access device fraud, in violation of 18 U.S.C. §1029(a)(2) (Count 1); 6 counts of aggravated identity theft, in violation of 18 U.S.C. § 1028A(a)(1) (Counts 2–5, 7–8); and 1 count of possession of 15 or more unauthorized access devices, in violation of 18 U.S.C. § 1029(a)(3) (Count 6). On the second day of trial, the district court granted the government's motion to dismiss Counts 2 and 3 on the grounds that Meme may have been a minor when the offenses were committed.

Testimony at trial revealed the following. Robert Novakowski, an investigator with JPMorgan Chase Bank, was investigating compromised debit cards following customer complaints. Novakowski received a list of compromised

debit cards and a list of transactions for those cards and obtained video surveillance of the person making the transactions. He testified that images captured on drive-up ATM cameras showed that Meme was making transactions with cards belonging to other people and with counterfeit payment cards. Some of those images showed Meme making transactions while driving a black Ford Mustang with a bumper sticker. Novakowski sought the assistance of law enforcement in identifying the person in the videos and images, and U.S. Secret Service Agent Sterling Posten identified that person as Meme. Novakowski conceded that he could not see the eye shape or eye color of the person in the images, but that the person had the same face as Meme and that he independently reviewed all photos and videos and, in so doing, was able to identify Meme as the person making the transactions.

Secret Service Agent Greg Narano testified that the Secret Service had obtained surveillance of people conducting unauthorized ATM withdrawals, one of whom was Meme. Accordingly, the Secret Service set up surveillance on several ATMs in an attempt to locate a black Mustang that was connected to some of these unauthorized withdrawals. While conducting surveillance, Narano saw a person driving a black Mustang with a bumper sticker use an ATM. Narano maintained surveillance, identified the person in the car as Meme, and took several photos of him. He followed Meme to Meme's father's house and continued his surveillance.

Narano conceded in cross-examination that the Mustang was not registered in Meme's name, that Meme's father owned the house, and that, based on his surveillance at the ATM, he was unable to determine the build of the person in the car or whether that person had facial hair. On redirect, he emphasized that he was able to identify the person in the Mustang as Meme because he had an unobstructed view of Meme's face at one point.

Secret Service Agent Ken Adams testified to the following. He, like Narano, was assigned to conduct surveillance at a Chase Bank ATM, saw a black Mustang pull up to the ATM, watched the driver commit a fraudulent transaction, identified the driver as Meme, and followed Meme to Meme's father's house. He also participated in Meme's arrest, after which he recovered two cell phones from the Mustang. On cross-examination, Adams conceded that there were no debit cards, credit cards, or large amounts of cash in the car when Meme was arrested.

Agent Posten then testified. He executed a search warrant of Meme's father's house and in one bedroom, recovered five plastic cards, a laptop, a firearm-training certificate in Meme's name, several pieces of unopened mail, and high school textbooks. Accordingly, Posten concluded that the bedroom belonged to Meme. In a room that he concluded belonged to Meme's brother, he recovered a plastic card, a personal check not belonging to anybody living in the house, a

money order, and a re-encoded plastic card.[1] In the living room of the house, Posten found a vehicle title belonging to Meme and traffic citations issued to Meme. He also found other pieces of mail, like bank records, that did not belong to anyone in the house—which he concluded was an indication of fraud taking place in the house. Posten conceded that the Mustang was a rental vehicle that was not rented by Meme; that according to the Florida Department of Highway Safety and Motor Vehicles, Meme did not live with his father; and that none of the cards in Meme's bedroom had been re-encoded.

Secret Service Agents Marcos Morales and Allen Thomasson testified that they had analyzed the phones recovered during Meme's arrest. Morales discovered that one of the phones was registered to a user identified as "MasonM1267." Thomasson's analysis of the text messages in the phones revealed that one of the phones had received text messages that identified the recipient (and thus, the phone owner) as Meme. He also reviewed the email account on the phone and discovered several emails received by an account belonging to "MasonM1267" and several emails containing credit and debit card

[1] In this context, re-encoding a plastic card serves to change the data on the card—in other words, from what source the card pulled funds or registered transactions—so that it no longer matched the information embossed on the card, *e.g.*, the name or displayed number. *See, e.g.*, *United States v. Cruz*, 713 F.3d 600, 608 (11th Cir. 2013) (discussing re-encoding credit and debit cards). Re-encoding cards is frequently charged as a violation of section 1029(a)(3), which prohibits the knowing, and with intent to defraud, possession of "devices which are counterfeit or unauthorized access devices." *E.g.*, *United States v. Grimon*, 923 F.3d 1302, 1306–1307 (11th Cir. 2019) (citing 18 U.S.C. § 1029(a)(3).

numbers. Thomasson also found data on the phone showing that the phone's owner had visited commercial background search websites (which are frequently used for identity theft and fraud) and disposable email service websites.

On the other phone, Thomasson also found information that identified Meme as the account owner—the phone had sent a picture of Meme's driver's license and the received texts referred to the phone's owner as Meme. He also discovered pictures of the Mustang, email accounts registered to "MasonM1267," debit card numbers and personal identification numbers, and correspondence relating to purchasing debit card numbers and PINs on the phone, and that the phone had visited commercial background search websites and websites for selling stolen card numbers.

Thomasson also testified that he analyzed the laptop recovered from what Posten had identified as Meme's room. He discovered that the computer's user account was "MasonM1627." He also found credit card and debit card numbers, the card-owners' personal information, software used to read and encode magnetic strips in cards, software used to read and encode card microchips, bank identification numbers, and bank routing numbers on the computer. All told, Thomasson estimated that hundreds of individuals' personal information and 120 different debit and credit card numbers were on Meme's laptop. He also discovered that the user of the laptop had visited websites selling credit card

numbers and commercial background search websites. On cross-examination, he conceded that he could not tell whether someone other than Meme had used the laptop and phones.

After the government rested its case, Meme moved for a judgment of acquittal. He argued that the government had failed to prove the existence of some of the victims named in the indictment, venue was improper, and some of the alleged criminal acts occurred while he was a minor. The district court denied Meme's motion.

Meme's case solely consisted of calling his stepmother, Willaine Amedee, who testified that Meme had never lived in his father's house or kept any belongings in the house. Meme rested, and then renewed his motion for a judgment of acquittal based on insufficient evidence. The district court again denied his motion.

The jury found Meme guilty of Counts 1 and 4–8. The district court sentenced Meme to a 39-month prison term, which consisted of 15-month concurrent sentences on Counts 1 and 6 and a 24-month sentence on Counts 4–5 and 7–8. Meme timely appealed to us.

ANALYSIS

On appeal, Meme argues that the evidence was insufficient to support his conviction. We review the sufficiency of the evidence *de novo*, "viewing the

evidence in the light most favorable to the government and drawing all reasonable inferences in favor of the verdict." *United States v. Schier*, 438 F.3d 1104, 1107 (11th Cir. 2006). The district court's denial of "motions for a judgment of acquittal will be upheld if a reasonable trier of fact could conclude that the evidence establishes the defendant's guilt beyond a reasonable doubt." *United States v. Rodriguez*, 218 F.3d 1243, 1244 (11th Cir. 2000). "[T]he issue is not whether a jury reasonably could have acquitted but whether it reasonably could have found guilt beyond a reasonable doubt," so we will not reverse a conviction solely because the defendant "put forth a reasonable hypothesis of innocence" at trial. *United States v. Campo*, 840 F.3d 1249, 1258 (11th Cir. 2016) (quotation omitted). We are bound by a jury's "rejection of the inferences raised by the defendant." *United States v. Hernandez*, 433 F.3d 1328, 1334–35 (11th Cir. 2005). Furthermore, we consider all evidence produced at trial against the defendant in evaluating his claim of insufficient evidence. *United States v. Thomas*, 8 F.3d 1552, 1558 n.12 (11th Cir. 1993).

An individual is guilty of access device fraud when he "knowingly and with intent to defraud traffics in or uses one or more unauthorized access devices during any one-year period, and by such conduct obtains anything of value aggregating $1,000 or more during that period." 18 U.S.C. § 1029(a)(2). An individual is guilty of possession of 15 or more unauthorized access devices if he possesses such

devices knowingly and with intent to defraud. *Id.* § 1029(a)(3). An individual is guilty of aggravated identity theft when he "knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person" during a felony violation of, among other things, "any provision contained in this chapter" relating to fraud. *Id.* §§ 1028A(a)(1), (c)(4). An "'access device' means any card, . . . account number, electronic serial number, . . . personal identification number, . . . or other means of account access that can be used, alone or in conjunction with another access device, to obtain money . . . or that can be used to initiate a transfer of funds." *Id.* § 1029(e)(1). An "'unauthorized access' device means any access device that is lost, stolen, . . . or obtained with intent to defraud." *Id.* § 1029(e)(3).

We read Meme's arguments on appeal as essentially arguing for a more favorable inference of the facts. He argues that fraud was taking place at his father's house (but he was not a part of it), that the Secret Service agents could not identify who used the phones or computer, that the ATM surveillance photos were poor-quality and did not lend themselves to identification, that no one described the physical characteristics of the person who was using the access devices, that Novakowski's identification of him was tainted, and that no counterfeit access devices were found in his "actual or constructive possession."

These arguments are unavailing. These arguments echo what Meme argued at trial—both to the district court and to the jury in his arguments for acquittal—

and the jury was entitled to reject those arguments and draw a different inference. We are not able to revisit the inference that the jury drew. *Hernandez*, 433 F.3d at 1334–35. In any event, we conclude that the evidence at trial was sufficient to support Meme's conviction for two reasons: (1) the phone and laptop evidence showed that Meme was committing access device fraud and (2) Meme was identified as the person committing access device fraud. We address each in turn.

First, the testimony at trial clearly showed—although somewhat circumstantially—that Meme was committing access device fraud. With regard to the phones, the agents testified that Meme visited commercial background search websites and websites where he could purchase stolen card numbers, had stolen card numbers stored on his phones, and had correspondence relating to his purchase thereof. The agents found similar evidence on Meme's laptop.

Meme does not, and cannot, seriously contest the evidence found on both devices—and so he instead suggests that *other* people were using the devices. We wholly reject this argument, because it requires us to substitute the jury's reasonable inference based on the evidence presented at trial for an unreasonable inference that happens to be more favorable to Meme. We think it is clear that the devices both belonged to, and were used by, Meme. Contrary to Meme's argument, the phones *were* found in his "actual or constructive possession," *i.e.*, the car he was driving at the time he was arrested. And while the laptop was found

in a room that Agent Posten had merely *identified* as Meme's room, the evidence certainly supports an inference that the room was Meme's. His argument that he did not live in the house, and thus that the room was not his, is strongly contradicted by the extent to which his belongings were found both in the room and elsewhere in the house. It is not likely that Meme's firearm-training certificate, vehicle title, and traffic citations would be in a house where he did not live. Finally, we find it significant that the user account on Meme's laptop was identical to the username of the email accounts on Meme's phones.

Second, Meme was identified as the person committing identity fraud. Though it is true that Novakowski's identification was at least partially predicated on Agent Posten's suggestion, we note that he testified that he independently reviewed all of the videos and images of the fraudulent ATM transactions and he provided an in-court identification of Meme. As we have explained previously, "[a]n in-court identification, even if preceded by a suggestive out-of-court identification procedure, is nevertheless admissible if the in-court identification has an independent source." *United States v. Cannington*, 729 F.2d 702, 711 (11th Cir. 1984).

But even if we concluded that Novakowski's identification of Meme was impermissible, we note that there are two additional—and more persuasive—witnesses who identified Meme. Both Agents Adams and Narano identified Meme

as the person in the black Mustang who made fraudulent transactions at an ATM. Their identification is significant—both were surveilling him and followed him to his father's house, and Adams participated in Meme's arrest.

Accordingly, we conclude that the evidence was sufficient to support Meme's conviction. The evidence as to the devices—both the phones in Meme's constructive possession at the time of his arrest and the laptop that was clearly Meme's—is persuasive evidence of Meme's fraud. And the identification of Meme, especially the eyewitness testimony of Secret Service agents who *saw* Meme committing access device fraud, is even more persuasive. We reject Meme's arguments to the contrary.

AFFIRMED.