NOT RECOMMENDED FOR FULL-TEXT PUBLICATION
File Name: 12a1274n.06

Nos. 11-2554, 11-2555, 11-2556

UNITED STATES COURT OF APPEALS
FOR THE SIXTH CIRCUIT

FILED
Dec 11, 2012
DEBORAH S. HUNT, Clerk

UNITED STATES OF AMERICA,	)	ON APPEAL FROM THE UNITED
	)	STATES DISTRICT COURT FOR THE
Plaintiff-Appellee,	)	WESTERN DISTRICT OF MICHIGAN
	)	
v.	)	
	)	
SHIFU LIN, (No. 11-2554)	)	
KANG HE, (No. 11-2555)	)	
ZHOU CHEN, (No. 11-2556)	)	
	)	
Defendants-Appellants.	)	

Before: COOK and WHITE, Circuit Judges; and SHARP, District Judge.[*]

HELENE N. WHITE, Circuit Judge. After a joint-jury trial, Defendants Shifu Lin, Kang He, and Zhou Chen (collectively, "Defendants") were convicted of conspiracy to commit fraud, 18 U.S.C. § 371, access-device fraud, 18 U.S.C. § 1029(a)(2), and aggravated identity theft, 18 U.S.C. § 1028A(a)(1). The district court sentenced Defendants to concurrent terms of 60 months' imprisonment and 78 months' imprisonment for the first two convictions, respectively, and 24 months' imprisonment for the third conviction, to be served consecutively to the sentences for the first two convictions. Defendants appeal, claiming that there was insufficient evidence to convict

[*]The Honorable Kevin H. Sharp, United States District Judge for the Middle District of Tennessee, sitting by designation.

them of aggravated identity theft, and that the court committed sentencing error in finding facts by a preponderance of the evidence at sentencing, improperly applying a two-level sentencing enhancement for the use of "sophisticated means," and calculating $500 of loss for credit-card numbers that Defendants possessed but did not use. We granted the government's motion to consolidate the three cases for briefing and submission. We AFFIRM.

I.

On January 11, 2011, a loss-prevention employee from a Meijer, Inc. grocery store ("Meijer") contacted the Kent County Sheriff's Department regarding a group of Asian males conducting suspicious credit-card transactions in the Grand Rapids, Michigan area. Meijer store employees reported that three men were repeatedly purchasing gift cards using multiple credit-card numbers and that some of these transactions were being declined. Meijer security reported the suspects' movement in real-time to police over the phone. Sheriff's deputies located a car that fit the description the Meijer employees had provided, followed it from one Meijer store to another, and eventually arrested Defendants after observing their behavior.

The deputies' search of the vehicle yielded more than 100 plastic gift cards with magnetic strips on the back, 72 of which had their magnetic strips re-encoded with stolen credit-card account numbers. These re-encoded gift cards allowed Defendants to use the cards as cloned credit cards to purchase new gift cards and other items. The deputies also found four laptop computers, two of which contained evidence that Defendants were purchasing credit-card account numbers online. A search of the laptops' files revealed several "data dumps" — files that contain numerous credit-card

account numbers and, in some cases, the names of the individuals whose names were on the accounts. Inside the laptop bags, the deputies found several Western Union wire-transfer receipts documenting multiple wire transfers to Russia and Ukraine. The deputies also found a magnetic strip reader/writer device hidden in the rear of the car that could re-encode the magnetic strips on the back of the gift cards with stolen credit-card account numbers. Further, each Defendant possessed two wallets containing gift cards that had been re-encoded with stolen credit-card numbers. Deputies found fake identification cards in the wallets of He ("Jie Gao") and Chen ("Chun Chen"). Deputies also found a Western Union receipt for a transfer of funds in the name of "Chun Chen" to an individual in Russia.

Records and video surveillance from Meijer showed that Defendants had visited numerous Meijer stores in the western Michigan area, purchasing gift cards and other items with stolen credit-card numbers. The credit-card account numbers on the Meijer records matched the unauthorized numbers found on the gift cards Defendants possessed, as well as the numbers found in the data dumps on Defendants' computers. When one of the credit cards was declined, Defendants would try another credit card in a back-to-back transaction. Meijer also produced video stills of Defendants purchasing Western Union wire transfers that were sent to Ukraine and Russia. An inspection of Defendants' computers revealed instant-message conversations between Defendants and unknown individuals in Russia and Ukraine, negotiating the purchase of credit-card numbers. Defendants were told by the sellers that the numbers had to be used within 24 hours or they would not work.

Prior to trial, Defendants entered into stipulations with the government agreeing that the account numbers listed in the indictment were valid credit-card numbers, possessed by actual

individuals who did not authorize Defendants to use their credit-card account number at any time. At trial, the court read the stipulations to the jury and instructed that it may assume the stipulated facts to be true. The court denied Defendants' motion for judgment of acquittal, finding that the combination of direct and circumstantial evidence, when viewed in the light most favorable to the government, would allow a jury to conclude beyond a reasonable doubt that Defendants were guilty of each charge of the indictment. Defendants presented no evidence and the jury returned a verdict of guilty on all counts as to all three Defendants.

The presentence report ("PSR") calculated the total offense level for each Defendant as 30, yielding a guideline range of 97 to 121 months under criminal history category I. To a base offense level of 6, U.S.S.G. § 2B1.1(a)(2), 14 levels were added because the loss involved was calculated as $857,937.74 (loss greater than $400,000 but less than $1,000,000). *Id*. at (b)(1)(H). The PSR added an additional six levels because the offense involved 250 or more victims, *Id.* at (b)(2)(C), and an additional two levels for the use of "sophisticated means." *Id.* at (b)(10)(C). Another two levels were added based on the possession or use of device-making equipment and production or trafficking of unauthorized access devices. *Id.* at (b)(11)(A)(i) and (B)(i). This gave each Defendant a total offense level of 30. In addition, 18 U.S.C. § 1028A(a)(1) mandates a consecutive two-year term of imprisonment for aggravated identity theft in addition to any other term of imprisonment imposed.

At sentencing, Defendants objected to the enhancements for more than 250 victims, and use of sophisticated means, and to the attribution of $500 of loss per unauthorized access device possessed. Defendants also moved for judgment of acquittal on the aggravated identity-theft conviction. Because all three Defendants raised these objections, the court consolidated a portion

of the sentencing hearing to resolve the common issues. The court denied the motion for acquittal, noting:

> [W]hile I understand that the defendants are protesting lack of knowledge that these numbers were assigned to individuals, I think it's also reasonably inferable from the totality of the evidence here that the means in which they acquired the numbers, that is through the Ukraine clandestinely, the guidance from individuals they were talking to that these numbers had a very short life span because fraudulent use would be detected quickly, I think that evidence also adds to the government's circumstantial case admittedly concerning the knowledge of the defendants . . .

The court sustained Defendants' objection to the number-of-victims calculation in the pre-sentence report[1] and overruled the objections regarding the use of sophisticated means and the calculation of the amount of loss. The resulting sentencing range was 78 to 97 months' imprisonment for counts one and two based on an offense level of 28.

After the joint portion of the sentencing hearing, the court held separate hearings on each Defendant's 18 U.S.C. § 3553(a) arguments. The court sentenced each defendant to a term of 60 months' imprisonment for conspiracy to commit fraud, 78 months' imprisonment for access-device fraud, to be served concurrently, and 24 months' imprisonment for aggravated identity theft, to be served consecutively to the sentences for conspiracy to commit fraud and access-device fraud. Defendants timely appealed.

---

[1]Regarding the number of victims, Defendants did not object to the 67 banks being counted as individual victims, but objected to the assumption that each credit-card number belonged to an individual person, and thus a separate victim, given that the government had not presented any evidence supporting this inference. The court agreed that the government had not proved that there were 250 victims. Accordingly, the six-level enhancement recommended by the PSR was reduced to four levels for involving 50 or more victims. *See* U.S.S.G. § 2B1.1(b)(2)(B).

II.

A. Sufficiency of the Evidence

This court reviews a challenge to the sufficiency of the evidence de novo. *United States v. Tocco*, 200 F.3d 401, 424 (6th Cir. 2000). The question on appeal is whether "after viewing the evidence in the light most favorable to the prosecution, *any* rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt." *Jackson v. Virginia*, 443 U.S. 307, 319 (1979) (emphasis in original). Circumstantial evidence alone can sustain a conviction and the evidence need not remove every reasonable hypothesis except that of guilt. *United States v. Stone*, 748 F.2d 361, 363 (6th Cir. 1984). The elements of aggravated identity theft are: (1) the defendant knowingly possessed a means of identification of another person (here, credit-card numbers); (2) the defendant knew that the means of identification belonged to another person; (3) the defendant knew that he had no lawful authority to possess the means of identification; and (4) the defendant possessed the means of identification during and in relation to the offense of access-device fraud. *See United States v. Adkins*, 372 F. App'x 647, 653 (6th Cir. 2010). Defendants only contest the second element, that they knew the means of identification belonged to another person.

In *Flores-Figueroa v. United States*, 556 U.S. 646 (2009), the Supreme Court held that the offense of aggravated identity theft requires proof that the defendant *knew* that the means of identification belonged to another person. *Id.* at 657. Defendants argue that the government did not present any affirmative evidence that they knew that the credit-card numbers they possessed

belonged to actual persons. Defendants argue that the government did not present any evidence proving that they had looked at the data-dump spreadsheets containing identifying information of the true holders of the credit-card numbers that were found on two of their computers. Defendants suggest that they were indifferent as to the source of the credit-card account numbers, and that this is not sufficient proof that they knowingly used a number belonging to another person.

However, Defendants do not contest that information identifying eleven individuals by name in conjunction with their credit-card numbers was found on their computer. This evidence is sufficient to support an inference that Defendants knew that at least some of the account numbers they purchased belonged to actual persons. Additionally, Defendants were told that the numbers had to be used within 24 hours, which the jury could view as notice that the account numbers belonged to the persons listed and might be reported stolen after 24 hours. Given that the evidence must be viewed in the light most favorable to the government, there was sufficient evidence to support Defendants' convictions of aggravated identity theft.

B. Due Process

Defendants argue that the district court violated their constitutional rights to due process of law and trial by jury by finding an amount of loss greater than $400,000 by a preponderance of the evidence at sentencing. This finding increased Defendants' offense level by 14 levels, thereby increasing the applicable guidelines range from 15–21 months to 78–97 months.

This court reviews a constitutional challenge to a sentence de novo. *United States v. Jones*, 641 F.3d 706, 713 (6th Cir. 2011). As Defendants acknowledge, this court has previously held that "judicial fact-finding in sentencing proceedings using a preponderance of the evidence standard post-*Booker* does not violate either Fifth Amendment due process rights, or the Sixth Amendment right to trial by jury." *United States v. Gates*, 461 F.3d 703, 708 (6th Cir. 2006). Therefore, we reject Defendants' challenge.

C. Sophisticated Means

Defendants argue that the district court erred by finding that their fraud was accomplished through the use of sophisticated means. When reviewing a district court's application of the sentencing guidelines, this court reviews factual findings for clear error and mixed questions of law and fact de novo. *United States v. Tolbert*, 668 F.3d 798, 800 (6th Cir. 2012). A factual finding is clearly erroneous when this court is left with "the definite and firm conviction that a mistake has been committed." *United States v. Lucas*, 640 F.3d 168, 173 (6th Cir. 2011).

The guidelines define "Sophisticated means" as:

> [E]specially complex or especially intricate offense conduct pertaining to the execution or concealment of an offense. For example, in a telemarketing scheme, locating the main office of the scheme in one jurisdiction but locating soliciting operations in another jurisdiction ordinarily indicates sophisticated means. Conduct such as hiding assets or transactions, or both, through the use of fictitious entities, corporate shells, or offshore financial accounts also ordinarily indicates sophisticated means.

U.S.S.G. § 2B1.1. cmt. n.8. "A series of criminal actions may constitute sophisticated means even if none of the offenses, standing alone, is especially complex or especially intricate." *United States v. Masters*, 216 F. App'x 524, 525 (6th Cir. 2007) (internal quotation marks omitted).

Defendants argue that their scheme was not very complex, and was in fact quite simple, especially when compared to other cases of access-device fraud. Defendants point to the fact that they did not hack into any computer and simply purchased the numbers online. Re-encoding gift cards was not difficult and the large volume of cards Defendants produced had more to do with repeating a simple process than with advanced technique. Defendants also argue that locating Meijer stores in the Midwest via a GPS was simple and did not reflect sophistication.

The government argues that Defendants purchased the credit-card numbers from individuals in Russia and Ukraine, then traveled from New York and Pennsylvania to Michigan to use the numbers, and that this cross-jurisdictional conduct is similar to the conduct in *United States v. Erwin*, 426 F. App'x 425 (6th Cir. 2011). In *Erwin*, the district court applied the sophisticated-means enhancement to a conspiracy where the defendants flew across the country to commit bank fraud. This court affirmed the application of the enhancement noting that "[t]his kind of cross-jurisdictional conduct, for the purposes of avoiding detection, is exactly the type of conduct described in the Guidelines definition of 'sophisticated means.'" *Id*. at 436.

In the instant case, Defendants purchased credit-card numbers over the internet from Ukraine and Russia before encoding them on used gift cards. Next, they traveled to the Midwest, far from their home states. They used the re-encoded gift cards to travel from Meijer store to

Meijer store, purchasing gift cards at self-checkout lanes, before moving on to new stores in order to evade detection. Once re-encoded, cards could be used like cash and there was no identifying information on the face of the card that would indicate that it contained a fraudulent credit-card number. While it may be true that individual steps in Defendants' conspiracy were not complicated, given the cross-jurisdictional conduct and technical knowledge necessary to commit the offense, the district court did not clearly err in concluding that the conspiracy as a whole reflected the use of sophisticated means.

D. Calculation of Loss

Defendants challenge the district court's interpretation of the guidelines as providing for a $500 loss amount per unauthorized access device, regardless of whether the device was actually used.

Section 2B1.1(b)(1) of the guidelines provides for an increase in offense level depending on how much loss the crime at issue caused. The text of Application Note 3(F)(i) reads:

> *Stolen or Counterfeit Credit Cards and Access Devices; Purloined Numbers and Codes*. — 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. However, if the unauthorized access device is a means of telecommunications access that identifies a specific telecommunications instrument or telecommunications account (including an electronic serial number/mobile identification number (ESN/MIN) pair), and that means was only possessed, and not used, during the commission of the offense, loss shall be not less than $100 per unused means.

U.S.S.G. § 2B1.1 cmt. n.3. Applying the greater of either the actual loss amount or $500 to each access-device number possessed by Defendants, the district court calculated a total loss of between $400,000 and $1 million, citing *United States v. Gilmore*, 431 F. App'x 428 (6th Cir. 2011), as controlling the calculation of loss. In *Gilmore*, the defendant challenged the calculation of loss on the basis that the district court applied the $500 per device calculation to access devices that the defendant possessed, but did not use. *Id.* at 429. This court rejected the defendant's argument, holding:

> The plain language of the note's first sentence imposes two clear conditions: (1) loss shall include any unauthorized charges made with the counterfeit access device or unauthorized access device, and (2) the loss shall not be less than $500 per access device. . . . The plain language sets a floor for calculating the loss attributable to each device, namely $500; it does not limit loss calculations to devices actually used.

Id. at 430; *see also United States v. Woods*, 367 F. App'x 607, 609 n.1 (6th Cir. 2010); *United States v. Little*, 308 F. App'x 633, 634 (3d Cir. 2009); *United States v. Camper*, 337 F. App'x 631, 632 (9th Cir. 2009).

Defendants do not dispute that *Gilmore* is controlling; rather they suggest that this court revisit *Gilmore*. Defendants cite no authority to support their argument, but urge that this court apply the rule of lenity. Because Defendants present no compelling reason to depart from *Gilmore*, we affirm the district court's calculation of loss.

III.

Accordingly, we AFFIRM.