F I L E D
United States Court of Appeals
Tenth Circuit

February 16, 2007

Elisabeth A. Shumaker
Clerk of Court

PUBLISH

UNITED STATES COURT OF APPEALS

TENTH CIRCUIT

UNITED STATES OF AMERICA, Plaintiff - Appellee, v. TODD A. WILLIS, Defendant - Appellant.	No. 06-6009

APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF OKLAHOMA
(D. Ct. No. CR-05-85-01-L)

Fred L. Staggs (Kent Eldridge, on the briefs), Oklahoma City, Oklahoma, appearing for Appellant.

Randal A. Sengel, Assistant United States Attorney (John C. Richter, United States Attorney, with him on the brief), Office of the United States Attorney, Oklahoma City, Oklahoma, appearing for the Appellee.

Before **TACHA**, Chief Circuit Judge, **SEYMOUR**, Circuit Judge, and **ROBINSON**,[*] District Judge.

TACHA, Chief Circuit Judge.

---

[*]Honorable Julie A. Robinson, United States District Judge for the District of Kansas, sitting by designation.

Defendant-Appellant Todd A. Willis was convicted of aiding and abetting the accessing without authorization of a protected computer, in violation of 18 U.S.C. §§ 2(a) and 1030(a)(2)(C), (c)(2)(B)(iii). He was sentenced to 41 months' imprisonment. He now appeals both his conviction and sentence. We take jurisdiction under 28 U.S.C. § 1291 and AFFIRM Mr. Willis's conviction, VACATE his sentence and REMAND for resentencing.

I. BACKGROUND

Mr. Willis was employed by Credit Collections, Inc., an Oklahoma City debt collection agency. To obtain information on individuals for debt collection, the agency utilized a financial information services website called Accurint.com—a site owned by LexisNexis. The information available on Accurint.com includes the names, addresses, social security numbers, dates of birth, telephone numbers, and other property data of many individuals. In order to access the information on Accurint.com, customers must contract with LexisNexis and obtain a username and password. In his position as a small claims supervisor, Mr. Willis had significant responsibility for the computers in the agency. As part of his employment, Mr. Willis assigned to employees usernames and passwords to access Accurint.com. Employees were not authorized to obtain information from Accurint.com for personal use. Mr. Willis deactivated the usernames and passwords of employees who no longer worked for the company.

While investigating two individuals, Michelle Fischer and Jacob Wilfong, for identity theft, police officers found pages printed out from Accurint.com with identifying information for many people. The information obtained from Accurint.com was used to make false identity documents, open instant store credit at various retailers, and use the store credit to purchase goods that were later sold for cash. A subpoena to Accurint.com revealed that the information had been obtained through the user name "Amanda Diaz," which was assigned to Credit Collections, Inc. Secret Service agents twice interviewed Mr. Willis about the identity theft. During the first interview, Mr. Willis insisted that the username and password assigned to Amanda Diaz had been deactivated and that there was no way to determine who had accessed the website. During the second interview, however, Mr. Willis admitted that he had given a username and password to his drug dealer in exchange for methamphetamine. He also admitted that he met Ms. Fischer through his drug dealer and that he began providing to her individuals' information he obtained through Accurint.com. After Ms. Fischer continued to ask Mr. Willis for information, he gave her the Amanda Diaz username and password so that she could access Accurint.com herself. On one occasion, when Ms. Fischer was having trouble accessing the site, Mr. Willis helped her to log on and specifically showed her how to obtain access to individuals' addresses, social security numbers, dates of birth, etc. In exchange, Ms. Fischer said that she would "take care of [Mr. Willis] later." She later gave him a silver Seiko watch.

When Mr. Willis learned through a newspaper article that Ms. Fischer had been arrested for identity theft, he deactivated the username and password.

Mr. Willis was charged in a one-count indictment alleging that he aided and abetted the accessing without authorization of a protected computer and obtaining information therefrom, in violation of 18 U.S.C. §§ 2(a) and 1030(a)(2)(C). Following a jury trial, Mr. Willis was convicted of the crime charged. In a special question submitted to the jury, the jury found beyond a reasonable doubt that the value of the information obtained by the unauthorized access exceeded $5,000. This finding set the maximum sentence under the penalty provisions of 18 U.S.C. § 1030(c)(2) at five years. Mr. Willis was sentenced to 41 months' imprisonment. He raises three issues on appeal. First, he argues that there was insufficient evidence that he knowingly, and with the intent to defraud, aided another in obtaining unauthorized access to a protected computer. Second, he argues that the District Court erred in failing to instruct the jury that to convict, it must find that Mr. Willis knowingly and intentionally aided another in obtaining information worth more than $5,000 or that it was foreseeable that the information obtained was worth more than $5,000. Finally, he argues that the District Court incorrectly applied the U.S. Sentencing Guidelines. We address each argument in turn.

II. DISCUSSION

A. Sufficiency of the Evidence

We review claims of insufficient evidence de novo. *United States v. Gurule*, 461 F.3d 1238, 1242 (10th Cir. 2006). "Evidence is sufficient to support a conviction if, viewing the evidence in the light most favorable to the government, a reasonable jury could have found the defendant guilty beyond a reasonable doubt." *United States v. LaVallee*, 439 F.3d 670, 697 (10th Cir. 2006). We will reverse a conviction "only if no rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt." *Gurule*, 461 F.3d at 1243 (quotation omitted). We also review questions of statutory interpretation de novo. *United States v. Begay*, 470 F.3d 964, 967 (10th Cir. 2006).

Under § 1030(a)(2)(C), "[w]hoever . . . intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer if the conduct involved an interstate or foreign communication . . . shall be punished as provided in subsection (c) of this section." Subsection (c) provides in relevant part that the punishment for a violation of § 1030(a) is:

> (2)(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), (a)(5)(A)(iii), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;
> (B) a fine under this title or imprisonment for not more than 5 years,

> or both, in the case of an offense under subsection (a)(2), or an attempt to commit an offense punishable under this subparagraph, if--
> . . .
> (iii) the value of the information obtained exceeds $5,000[.]

18 U.S.C. § 1030(c)(2)(A)–(B). In other words, the crime of intentionally accessing a protected computer without authorization and thereby obtaining information from that computer is punished as a misdemeanor unless, *inter alia*, the value of the information obtained exceeds $5,000, in which case it is a felony.

Mr. Willis argues that Congress could not have intended that any person who intentionally aids another in gaining unauthorized access to a protected computer be prosecuted as a felon if the information the third party obtains has a value of more than $5,000. Rather, he argues, the person who aids and abets must have the intent to defraud in so doing and must know that the information obtained will have such a value. To this end, he maintains that there was no proof that Mr. Willis knew that Ms. Fischer would use the information she obtained from Accurint.com to commit identity theft—the evidence established only that he thought he was helping her obtain information on people who owed her money. We reject Mr. Willis's arguments and conclude that § 1030(a)(2)(C) only requires proof that the defendant intentionally accessed information from a protected computer; the section does not require proof of intent to defraud nor proof that the defendant knew the value of the information obtained.

"[I]n order to be convicted of aiding and abetting, a defendant must share

in the intent to commit the underlying offense." *United States v. Vallejos*, 421 F.3d 1119, 1123 (10th Cir. 2005) (alterations and quotation omitted). To be convicted of the underlying offense, 18 U.S.C. § 1030(a)(2)(C), a defendant must "intentionally access[] a computer without authorization or exceed[] authorized access, and thereby obtain . . . information from any protected computer . . . ." Mr. Willis insists that the intent to defraud is an element of § 1030(a)(2)(C) because it is such an element under § 1030(a)(4). Under that section:

> Whoever . . . knowingly *and with intent to defraud*, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period, . . . shall be punished as provided in subsection (c) of this section.

18 U.S.C. § 1030(a)(4) (emphasis added).

A plain reading of the statute reveals that the requisite intent to prove a violation of § 1030(a)(2)(C) is not an intent to defraud (as it is under (a)(4)), it is the intent to obtain unauthorized access of a protected computer. *See Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121, 1125 (W.D. Wash. 2000) (one element "under § 1030(a)(4) that is not present under § 1030(a)(2)(C) is the intent to defraud"). That is, to prove a violation of (a)(2)(C), the Government must show that the defendant: (1) intentionally accessed a computer, (2) without authorization (or exceeded authorized access), (3) and thereby obtained information from any protected computer if the conduct

involved an interstate or foreign communication. The government need not also prove that the defendant had the intent to defraud in obtaining the information or that the information was used to any particular ends.[1]

Nevertheless, Mr. Willis contends, without citation to authority, that subsection (a)(2)(C) is the general provision of the statute and that subsection (a)(4) is the specific provision of the statute. That is, he argues, subsection (a)(4) sets out the specific elements required to prove a violation of subsection (a)(2)(C), and his conduct should be judged under subsection (a)(4), requiring an intent to defraud. We disagree.

As an initial matter, other courts have explained that each subsection of § 1030 addresses a different type of harm. *See P.C Yonkers, Inc. v. Celebrations the Party and Seasonal Superstore*, 428 F.3d 504, 510 (3d Cir. 2005) ("18 U.S.C. § 1030 lists seven different types of conduct punishable by fines or imprisonment."); *Register.com, Inc. v. Verio, Inc.*, 126 F. Supp. 2d 238, 251

---

[1]The legislative history of § 1030(a)(2)(C) supports our plain reading of the statute. In 1986, Congress changed the intent standard in § 1030(a)(2) from "knowingly" to "intentionally." In so doing, the Senate emphasized that "intentional acts of unauthorized *access*—rather than mistaken, inadvertent, or careless ones—are precisely what the Committee intends to proscribe." S. Rep. No. 432, 99th Cong., 2d Sess., *reprinted in* 1986 U.S.C.C.A.N. 2479, 2483 (emphasis added). The "'intentional' standard is designed to focus Federal criminal prosecutions on those whose conduct evinces a clear *intent to enter*, without proper authorization, *computer files or data belonging to another*." *Id.* at 2484 (emphasis added). The Senate report refers to § 1030(a)(2) as an "unauthorized access offense." *Id.* at 2488.

(S.D.N.Y. 2000), *aff'd in part and reversed in part on other grounds*, 356 F.3d 393 (2d Cir. 2004). For example, subsection (a)(2)(C) requires that a person intentionally access a computer without authorization and thereby *obtain information*, whereas subsection (a)(5)(C) requires that a person intentionally access a computer without authorization and thereby *cause damage*. *Register.com*, 126 F. Supp. 2d at 251. Similarly, subsection (a)(4) has different elements than subsection (a)(2)(C). In addition to requiring that a person act with the specific intent to defraud, a violation of (a)(4) also differs from (a)(2)(C) in that a person can violate the former by obtaining "*anything of value*" by the unauthorized access, whereas, as noted above, a person violates (a)(2)(C) by obtaining "*information*."

Furthermore, subsections (a)(2)(C) and (a)(4) are punished differently. Under § 1030(c), a violation of subsection (a)(2) is punishable by no more than one year in prison unless, *inter alia*, the value of information obtained exceeds $5,000, in which case the offender is subject to up to five years' imprisonment. *See* 18 U.S.C. § 1030(c)(2). On the other hand, a violation of (a)(4) subjects a person to five years' imprisonment if the defendant obtains anything of value—regardless of its value—unless the thing obtained is merely the "use of the computer and the value of such use is not more than $5,000 in any 1-year period." *Id.* at § 1030(c)(3). In other words, if a person knowingly and with the intent to defraud accesses a protected computer and by means of such conduct furthers the

intended fraud and obtains information valued at only $1,000, for example, he would nevertheless be subject to the stricter penalty provided for under § 1030(c)(3). The difference between the subsections is the type of intent required.

Finally, we reject Mr. Willis's argument that the statute requires proof that the defendant knew the value of the information obtained. There is no separate intent or knowledge requirement with respect to the penalty provision of the statute, § 1030(c). The relevant portion of the statute provides that "punishment for an offense under subsection (a) or (b) of this section is . . . a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2) . . . if . . . the value of the information obtained exceeds $5,000." 18 U.S.C. § 1030(c)(2)(B)(iii). The defendant need not know that the value of the information obtained has a particular value, or any value, for that matter.

Mr. Willis does not contest that he provided Ms. Fischer unauthorized access to Accurint.com. He merely argues that he had no intent to defraud in so doing nor did he know that she planned to obtain information of a certain value. As the foregoing discussion demonstrates, however, such proof is not required to establish a violation of § 1030(a)(2)(C). Accordingly, his sufficiency of the evidence argument fails.

B. Jury Instructions

We review a jury instruction for plain error when a party fails to object to the instruction at trial. *LaVallee*, 439 F.3d at 684. Mr. Willis's argument with respect to the jury instructions is essentially a reiteration of his sufficiency of the evidence argument. He contends the District Court should have instructed the jury that to find Mr. Willis guilty of aiding and abetting, the Government must prove beyond a reasonable doubt that Mr. Willis "knew or intended that the information obtained as the result of the unauthorized access exceeded $5,000." We have just held, however, that the intent requirement in § 1030(a)(2)(C) respects obtaining unauthorized access to a protected computer. The intent requirement does not extend to the value of the information ultimately obtained. Accordingly, the District Court did not commit plain error in giving the jury instructions.

C. Sentencing

Following Mr. Willis's conviction, the probation office prepared a presentence report ("PSR"). The United States Sentencing Commission guideline for a violation of § 1030(a)(2) is found at U.S. Sentencing Guidelines Manual ("U.S.S.G." or "Guidelines") § 2B1.1 and calls for a base offense level of 6. *See* U.S.S.G. § 2B1.1(a)(2). The probation office recommended a 10-level enhancement under § 2B1.1(b)(1)(F) after concluding that the total amount of loss from Ms. Fischer and her co-conspirators' identity theft was more than $120,000. It also recommended a 2-level enhancement under § 2B1.1(b)(10)(C)(i) because it

concluded the offense involved "the unauthorized transfer or use of any means of identification unlawfully to produce or obtain any other means of identification." Finally, it recommended a 2-level enhancement under § 3B1.3 because Mr. Willis abused his position of trust by giving others access to the personal credit information of the victims in this case. Given these enhancements, the PSR calculated Mr. Willis's base offense level at 20. The probation office also determined that based on Mr. Willis's two prior felony convictions for embezzlement by an employee, a prior felony conviction for uttering a forged instrument, and a prior misdemeanor conviction for driving under the influence and driving under suspension, he had a criminal history category of V. The recommended Guidelines range for an offense level of 20 and a criminal history category of V is 63 to 70 months. *See* U.S.S.G. § 5 Pt. A. Because the statutory maximum for the offense is five years, however, the PSR noted that Mr. Willis cannot receive a sentence longer than 60 months.

Mr. Willis filed several objections to the PSR. Relevant to this appeal, Mr. Willis contended that he should not be held accountable for the total loss resulting from his passing on a username and password to others. He argued that it was not foreseeable to him, nor did he intend, that *any* loss would result from his actions. He also argued that because he did not share Ms. Fischer's fraudulent intent to steal identities, the § 2B1.1(b)(10)(C)(i) enhancement did not apply. At the sentencing hearing, the Government agreed with Mr. Willis to the extent that he

argued the entire amount of loss should not be attributed to Mr. Willis for sentencing purposes. It took the position that only those losses directly caused by Ms. Fischer were attributable to Mr. Willis, which were losses of more than $10,000 but less than $30,000.

The District Court agreed with the Government and found Ms. Fischer's conduct foreseeable to Mr. Willis. It therefore imposed a 4-level enhancement on Mr. Willis's base offense level (as opposed to the 10-level enhancement recommended by the PSR). *See* U.S.S.G. § 2B1.1(b)(1)(C). It also applied the § 2B1.1(b)(10)(C)(i) enhancement because the offense involved using a means of identification to produce another means of identification, as well as the § 3B1.3 enhancement because Mr. Willis abused a position of trust. This produced an adjusted offense level of 14, which, when coupled with his criminal history category of V, resulted in an advisory Guidelines range of 33 to 41 months, *see* U.S.S.G. § 5 Pt. A. The District Court sentenced Mr. Willis to 41 months' imprisonment.

On appeal, Mr. Willis renews his claim that the District Court erred in enhancing his sentence based on the conclusion that any loss caused by Ms. Fischer was foreseeable to him. He contends that the evidence established only that he thought Ms. Fischer was going to use the information to track down people who owed her money, and not to engage in the type of criminal venture in which she involved herself. He also contends that the District Court erred in

imposing the enhancement under § 2B1.1(b)(10)(C)(I) for "unauthorized transfer or use of any means of identification unlawfully to procure or obtain other means of identification."

_____1. Standard of Review

We apply a two-step approach to appellate review of sentences. *United States v. Herula*, 464 F.3d 1132, 1136 (10th Cir. 2006). "First, we determine whether the district court correctly calculated the applicable guideline range." *Id.* If so, then we determine whether the sentence imposed is "reasonable." *Id.* A sentence within the correctly calculated Guidelines range is entitled to a rebuttable presumption of reasonableness. *United States v. Kristl*, 437 F.3d 1050, 1055 (10th Cir. 2006). We continue to review legal questions de novo and the district court's factual findings for clear error. *Herula*, 464 F.3d at 1136.

_____2. Section 2B1.1(b)(1)(C)

In determining the amount of loss associated with an offense for purposes of § 2B1.1(b), courts must consider "the greater of the actual or intended loss." U.S.S.G. § 2B1.1 cmt. n.3(A). "Actual loss," which is the only loss relevant here, "means the reasonably foreseeable pecuniary harm that resulted from the offense." *Id.* at cmt. n.3(A)(i). And, "'reasonably foreseeable pecuniary harm' means pecuniary harm that the defendant knew or, under the circumstances, reasonably should have known, was a potential result of the offense." *Id.* at cmt. n.3(A)(iv).

The record adequately supports the District Court's conclusion that it was foreseeable to Mr. Willis that the information obtained by Ms. Fischer from Accurint.com would have a value of between $10,000 and $30,000. Prior to disseminating the username and password to Ms. Fischer, Mr. Willis gave his methamphetamine supplier a username and password. He did this "in exchange for a better price on ice or crystal meth." This shows that Mr. Willis knew that the information available on the website was valuable. So, too, when Mr. Willis gave Ms. Fischer a username and password, she assured him that she would "take care of [him] later." He also said that he did not provide her access to the website out of his own personal greed—if greed was the motivating factor, he "would be living high right now and could have nice things." Again, this shows that Mr. Willis was well aware that the information available on the website was valuable. As such the District Court's conclusion that Mr. Willis knew or should have known that more than $10,000 and less than $30,000 of pecuniary harm could have resulted from his offense is not clearly erroneous.

_____3. Section 2B1.1(b)(10)

Section 2B1.1(b)(10)(C)(i) instructs a court to enhance a defendant's sentence by two levels "[i]f the offense involved . . . the unauthorized transfer or use of any means of identification unlawfully to produce or obtain any other means of identification." The offense for which Mr. Willis was convicted did not include this type of act—he was convicted of providing unauthorized access to a

protected computer. But "offense" for purposes of the Guidelines "means the offense of conviction and all relevant conduct under § 1B1.3." U.S.S.G. § 1B1.1 cmt. n.1(H). Relevant conduct includes:

> (1) (A) all acts and omissions committed, aided, abetted, counseled, commanded, induced, procured, or willfully caused by the defendant; and
>
> (B) in the case of a jointly undertaken criminal activity (a criminal plan, scheme, endeavor, or enterprise undertaken by the defendant in concert with others, whether or not charged as a conspiracy), all reasonably foreseeable acts and omissions of others in furtherance of the jointly undertaken criminal activity,
>
> that occurred during the commission of the offense of conviction, in preparation for that offense, or in the course of attempting to avoid detection or responsibility for that offense[.]

U.S.S.G. § 1B1.3(a). The Guidelines provide examples of when these provisions are properly applied. For instance:

> Defendant C is the getaway driver in an armed bank robbery in which $15,000 is taken and a teller is assaulted and injured. Defendant C is accountable for the money taken under subsection (a)(1)(A) because he aided and abetted the act of taking the money (*the taking of money was the specific objective of the offense he joined*). Defendant C is accountable for the injury to the teller under subsection (a)(1)(B) because the assault on the teller was in furtherance of the jointly undertaken criminal activity (the robbery) and was reasonably foreseeable in connection with that criminal activity (given the nature of the offense).

U.S.S.G. § 1B1.3, app. n.2, illus. (b)(1) (emphasis added). In sum, subsection (a)(1)(A) applies when the defendant aids and abets another person in committing the "specific objective of the offense," while subsection (a)(1)(B) applies to the

conduct of others "in furtherance of the jointly undertaken criminal activity" that is reasonably foreseeable to the defendant.[2]

Using the information obtained from Accurint.com to create false identifications was not part of the "specific objective of the offense" for which Mr. Willis was convicted. As such, this is not properly chargeable to Mr. Willis under § 1B1.3(a)(1)(A).

Under § 1B1.3(a)(1)(B), "the 'scope of the agreement' and 'reasonable foreseeability' are independent and necessary elements of relevant conduct." *United States v. Green*, 175 F.3d 822, 837 (10th Cir. 1999) (quotation omitted). Thus, for § 1B1.3(a)(1)(B) to apply, a district court "'must first determine . . . the scope of the specific conduct and objectives embraced by the defendant's agreement,'" *United States v. Melton*, 131 F.3d 1400, 1404 (10th Cir. 1997) (alteration in original) (quoting U.S.S.G. § 1B1.3 cmt. n.2), because "a defendant's accountability only extends to the criminal activity he agreed to undertake," *United States v. Dazey*, 403 F.3d 1147, 1176 (10th Cir. 2005). The commentary to § 1B1.3 explains:

> [T]he scope of the criminal activity jointly undertaken by the defendant (the "jointly undertaken criminal activity") is not necessarily the same as the scope of the entire conspiracy, and hence

---

[2]Subsections (a)(1)(A) and (a)(1)(B) are not mutually exclusive. *See* U.S.S.G. 1B1.3, app. n.2, illus. (a)(1). But, "[t]he requirement of reasonable foreseeability applies only in respect to the conduct . . . of others;" it "does not apply to conduct that the defendant personally undertakes, aids, [or] abets." U.S.S.G. § 1B1.3 cmt. app. n.2.

> relevant conduct is not necessarily the same for every participant. In order to determine the defendant's accountability for the conduct of others under subsection (a)(1)(B), the court must first determine the scope of the criminal activity the particular defendant agreed to jointly undertake (*i.e.*, the scope of the specific conduct and objectives embraced by the defendant's agreement).

U.S.S.G. § 1B1.3 cmt. app. n.2. This means that "at sentencing the district court must make particularized findings tying the defendant to the relevant conduct used to increase the base level offense." *Green*, 175 F.3d at 837. The court must then also conclude that the conduct of others "in furtherance of the criminal activity jointly undertaken by the defendant" was "reasonably foreseeable in connection with that criminal activity." U.S.S.G. § 1B1.3 app. n.2.

Even if we conclude that it was foreseeable to Mr. Willis that Ms. Fischer would use the Accurint.com username and password in the manner in which she did, the District Court failed to make particularized findings about the scope of the criminal activity to which Mr. Willis agreed. In applying the enhancement, the District Court said only that "based upon the information that the Court has from the trial and the evidence" the enhancement was proper—though it had earlier said:

> [T]he Court . . . is well aware of all of the other parties and the roles they played in . . . [the identity theft conspiracy], and my information is that the probation office simply put this in [the PSR] for background as to the overall conspiracy in which Mr. Willis's actions related to, while he was not a part of the conspiracy or charged as being a part of the conspiracy, the end result of his actions, and it has no . . . impact on the guidelines.

This appears to suggest that the District Court did not find Mr. Willis to have jointly undertaken to aid and abet the identity theft portion of the crime. In fact, Ms. Fischer testified at trial that she deceived Mr. Willis and told him that she wanted access to Accurint.com so that she could track down people who owed her money. There was no evidence to suggest that Mr. Willis was actually aware of Ms. Fischer's fraudulent activities until he read a newspaper article about it. Again, even if Ms. Fischer's identity theft scheme was reasonably foreseeable to Mr. Willis, "[r]elevant conduct is limited to those reasonably foreseeable [acts] that are part of the criminal activity [the defendant] agreed to jointly undertake." *United States v. McClatchey*, 316 F.3d 1122, 1128 (10th Cir. 2003) (internal quotation marks omitted). "'[T]he fact that the defendant is aware of the scope of the overall operation is not enough to [establish the scope of the defendant's agreement] and therefore, is not enough to hold him accountable for the activities of the whole operation.'" *Id.* at 1129 (quoting *United States v. Campbell*, 279 F.3d 392, 400 (6th Cir. 2002)) (second alteration in original). Because the District Court failed to make particularized findings about the scope of the criminal activity Mr. Willis agreed to jointly undertake, we remand the case for further factual findings. *See Green*, 175 F.3d at 837 (remanding for factual findings on the scope of the criminal activity jointly undertaken when the district

court failed to make "particularized findings").[3]

III. CONCLUSION

For the foregoing reasons, we AFFIRM Mr. Willis's conviction and REMAND to the District Court with instructions to VACATE his sentence and resentence him in accordance with this opinion.

[3]Mr. Willis also argues that the question of his knowledge and intent with regard to the identity thefts and the specific amount of loss should have been submitted to a jury pursuant to *Apprendi v. New Jersey*, 530 U.S. 466 (2000). Defendant's reliance is misplaced. In certain circumstances, *Apprendi* requires a factor that can increase the defendant's sentence to be found by the jury beyond a reasonable doubt. *Id.* at 489. "*Apprendi*[, however,] does not apply to sentencing factors that increase a defendant's guideline range but do not increase the [sentence beyond the] statutory maximum." *United States v. Sullivan*, 255 F.3d 1256, 1265 (10th Cir. 2001). As determined by the jury, the statutory maximum for Mr. Willis's offense is five years. Because his sentence was 41 months, *Apprendi* does not apply.