United States Court of Appeals
For the First Circuit

Nos. 22-1297, 22-1609

UNITED STATES OF AMERICA,

Appellee,

v.

PAUL IWUANYANWU,

Defendant, Appellant.

APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

[Hon. Denise J. Casper, U.S. District Judge]

Before

Gelpí, Lynch, and Thompson,
Circuit Judges.

Christine DeMaso, Assistant Federal Public Defender, for appellant.

Alexia R. De Vincentis, Assistant United States Attorney, with whom Rachael S. Rollins, United States Attorney, was on brief, for appellee.

May 30, 2023

GELPÍ, Circuit Judge. Appellant Paul Iwuanyanwu ("Iwuanyanwu") participated in two fraud schemes, business email compromise ("BEC") and online romance, for which he pled guilty to one count of conspiracy to commit wire fraud, two counts of wire fraud, one count of conspiracy to commit mail fraud, one count of mail fraud, and one count of engaging in monetary transactions in property derived from specified unlawful activity ("unlawful monetary transactions"). The district court, considering the unauthorized use of a third-party identity and the substantial financial hardship caused to one of the victims, sentenced Iwuanyanwu to thirty months imprisonment, which represented a downward variance from the Guidelines Sentencing range. Iwuanyanwu now challenges the district court's imposition of two Sentencing Guidelines enhancements: (1) the unauthorized use of a means of identification unlawfully to produce another means of identification and (2) substantial financial hardship caused to one of the victims. For the reasons discussed below, we affirm.

I. Background

Relevant Facts

Because this appeal follows a guilty plea, we draw the facts from the uncontested portions of the Presentence Report ("PSR") and the transcript of the sentencing hearing. United States v. Bishoff, 58 F.4th 18, 20 n.1 (1st Cir. 2023). First, we introduce what a business email compromise ("BEC") scheme is; next,

we outline the conspiracy against specific victims. Finally, we review the procedural history of the case before appeal.

BEC Fraud Scheme

From April 2017 through March 2019, Iwuanyanwu engaged in a BEC scheme. BEC scams involve fraudulent business transactions conducted via wire transfer payments. The fraud is carried out by compromising and/or "spoofing" legitimate business email accounts through computer intrusion techniques, such as phishing, with the goal of inducing employees at a targeted company to transfer funds without authorization, most often to accounts controlled by the perpetrators of the scheme. Here, the spoofed email addresses looked almost exactly like the email addresses belonging to the victims.

Funds Diverted from Russian Company

On approximately May 21, 2018, Victim Company 1 (a custom tube and pipe manufacturer based in Illinois) emailed Victim Company 3 (a construction company based in Moscow, Russia) an invoice for $888,274 pursuant to a contract between both. Because Victim Company 1's email had at some point been compromised, the email and attachment were redirected to emails controlled by the co-conspirators. One or more co-conspirators then altered the attached invoice, by adding payment instructions, and subsequently sent the altered invoice to Victim Company 3 from a spoofed email account. The altered invoice instructed Victim Company 3 to wire

payments to a Regions Bank account opened by one of Iwuanyanwu's co-conspirators. Prior to the transfer, however, Regions Bank closed the account.

As a result of the account's closure, on or about July 6, 2018, Iwuanyanwu opened an account at a Bank of America branch in Medfield, Massachusetts in the name of Victim Company 1. Iwuanyanwu falsely listed himself as the owner of the business, the sole account holder, and the only authorized signer. On approximately July 9, 2018, one or more of the co-conspirators, pretending to be Victim Company 1, sent a new invoice to Victim Company 3 instructing the company to transfer $884,274 to the newly opened Bank of America account. A week later, Victim Company 3 wired $884,274 from its bank in Russia to the Bank of America account that Iwuanyanwu had recently opened. A day later, Iwuanyanwu transferred $95,320 from the Bank of America account to a Citibank, N.A. account in New York, held by a Nigerian bank.

Funds Diverted from Pakistani Company

Later that year, on approximately October 18, 2018, an individual posing as S.P.[1] used a false Florida driver's license to open a Branch Banking and Trust ("BB&T") account in the name of S.P. DBA Quantek Renovation ("S.P. DBA" or "S.P. account"). A real person, posing as S.P., used S.P.'s actual birth date and

[1] Initials are used throughout to protect the victim's identity.

social security number to open the account. The real S.P. did not know about or authorize the use of his identity and personal identifying information. From approximately November 17 to November 19, 2018, Iwuanyanwu exchanged WhatsApp messages with a co-conspirator who identified himself as "More Blessing 1" in the messaging platform. They exchanged information about the S.P. DBA account.

On approximately November 27, 2018, a WhatsApp user identified as "Motorola 1" notified Iwuanyanwu that Victim Company 4 (a Pakistani textile company) made a wire transfer to the S.P. account. From approximately November 27 to December 5, 2018, the S.P. account received eight international transfers totaling $164,327. BB&T closed the account shortly thereafter.

Attempted Diversion of Funds from Victim Company 6

On or about July 19, 2018, a co-conspirator sent Iwuanyanwu a WhatsApp message stating the name of Victim Company 6. That same day, Iwuanyanwu went to a Santander Bank branch and opened an account in the name of Victim Company 6, which he attested to being the owner of. Although a co-conspirator later sent a spoofed email to a customer of Victim Company 6 with instructions on how to remit payment via wire transfer, no funds were ever wired to said Santander Bank account.

Online Romance Fraud Scheme

From around 2016 through January 2020, Iwuanyanwu, and one or more co-conspirators, conspired to defraud victims that they encountered on online dating sites by persuading them to send and/or receive money on their behalf. Iwuanyanwu, and one or more co-conspirators, cashed and withdrew funds from the accounts to which victim funds were sent.

Victim A

In connection with this scheme, from March 2018 through approximately January 2020, Iwuanyanwu persuaded Victim A (who allegedly was his long-time girlfriend at the time) to open several bank accounts for him to receive transfers that he claimed were for a car business. Victim A opened a Crescent Credit Union account in her own name and another account at Citizens Bank in the name of WJ Export. The latter was used in connection with Victim B.

Victim B

In or about February and March 2019, an individual using the identity "Sergey Vince" (not Iwuanyanwu or the named co-conspirator), who was in an online romantic relationship with Victim B, told Victim B that he was traveling for work and needed some money because he ran short of funds. Victim B, a disabled and unemployed woman, agreed to help him out. "Sergey" then provided her the account information for the WJ Export Citizens Bank account that had been opened by Victim A at Iwuanyanwu's

direction. Between February 20, 2019, and March 6, 2019, at "Sergey's" request, Victim B sent $6,000 via two $3,000 wire transfers. Between February 21-22, 2019, Iwuanyanwu made five separate withdrawals of $600 cash from the account that Victim B had sent money to. On or about March 6, 2019, Iwuanyanwu asked Victim A to accompany him to the bank to withdraw $3,000 from the account that she had opened for him. Later that day, Iwuanyanwu and Victim A went to the bank and withdrew the $3,000.

Victim C

Beginning in 2016, Victim C engaged in an online relationship with an individual (not Iwuanyanwu) who she believed was in Africa. Between April and November 2018, Victim C was fraudulently induced to send funds to various bank accounts in Ghana and Nigeria, totaling more than $10,000. On or about February 28, 2019, Iwuanyanwu deposited into his personal bank account a money order for $500 that Victim C had sent one of his co-conspirators the day before. About a week later, following the commands of one of Iwuanyanwu's co-conspirators, Victim C sent via United States mail a $500 money order to Iwuanyanwu's Medfield address. Victim C believed she was sending the money to help pay her online friend's rent.

Procedural Background

In April 2019, a grand jury indicted Iwuanyanwu and a co-conspirator (not a party to this appeal), charging them each

with one count of conspiracy to commit wire fraud related to the BEC scheme, one count of wire fraud, and charging Iwuanyanwu with one count of engaging in an unlawful monetary transaction. However, in July 2020, the grand jury issued a six-count superseding indictment against Iwuanyanwu charging him with conspiracy to commit wire fraud, in violation of 18 U.S.C. § 1349; two counts of wire fraud, in violation of 18 U.S.C. § 1343; conspiracy to commit mail fraud, in violation of 18 U.S.C. § 1349; mail fraud, in violation of 18 U.S.C. § 1341; and unlawful monetary transactions, in violation of 18 U.S.C. § 1957. On October 27, 2021, Iwuanyanwu pled guilty to all six counts of the superseding indictment.

The parties and the Probation Office agreed that Iwuanyanwu's criminal history category was I, his base offense level was seven, a fourteen-point enhancement applied because of the loss amount, and a three-point deduction applied for acceptance of responsibility. The PSR added a two-point enhancement pursuant to U.S.S.G. § 2B1.1(b)(11)(A)(ii) because Iwuanyanwu used fraudulent certificates of incorporation to open the bank accounts. He objected. In response to Iwuanyanwu's objection to the § 2B1.1(b)(11)(A)(ii) enhancement, the Amended PSR instead applied an enhancement for unauthorized use of a means of identification on subsection (C)(i) because a member of the conspiracy used S.P.'s identity to open a bank account. The

Amended PSR also added a two-point enhancement under U.S.S.G. § 2B1.1(b)(2)(A)(iii) based on the substantial financial hardship Victim B endured. Iwuanyanwu objected to both enhancements in his sentencing memorandum.

At the sentencing hearing, the district court adopted the Amended PSR's Guideline calculation, overruling Iwuanyanwu's objections to both enhancements. The applicable sentencing range was forty-one to fifty-one months. The district court, however, sentenced him, by way of a downward variance, to thirty months imprisonment, followed by two years of supervised release. Iwaunyanwu timely appealed.

II. Standard of Review

We review preserved challenges to the district court's application of Sentencing Guidelines enhancements for abuse of discretion. United States v. Ilarraza, 963 F.3d 1, 7 (1st Cir. 2020). However, this standard is not "monolithic." Id. Thus, "our review . . . consists of 'clear error review [of] factual findings, de novo review [of] interpretations and applications of the [G]uidelines, and abuse of discretion review [of] judgment calls.'" United States v. Kitts, 27 F.4th 777, 789 (1st Cir. 2022) (alterations in original) (quoting United States v. O'Brien, 870 F.3d 11, 15 (1st Cir. 2017)).

III. Discussion

Enhancement for Unauthorized Use of Means of Identification

Iwuanyanwu challenges the district court's application of a two-point enhancement under U.S.S.G. § 2B1.1(b)(11)(C)(i) related to the use of S.P.'s identity. He asserts that it was not foreseeable to him that the conspiracy would use the identity of a third party (S.P.'s name, birth date, and social security number), who was not involved in the scheme, to fraudulently open a bank account. He further contends that the government did not prove that he knew or should have known that the bank account was not opened by S.P.

The enhancement at issue here provides for a two-point increase for "the unauthorized transfer or use of any means of identification unlawfully to produce or obtain any other means of identification[.]" U.S.S.G. § 2B1.1(b)(11)(C)(i). The Guidelines' commentary clarifies that it "applies in a case in which a means of identification of an individual other than the defendant (or a person for whose conduct the defendant is accountable under § 1B1.3 (Relevant Conduct)) is used without that individual's authorization unlawfully to produce or obtain another means of identification." Id. cmt. n.10(C)(i). A means of identification, such as a name, social security number, date of birth, or any other personal identification number, see 18 U.S.C.

§ 1028(d)(7), "shall be of an actual (i.e., not fictitious) individual, other than the defendant," U.S.S.G. § 2B1.1 cmt. n.1. For example, a defendant who obtains a bank loan using an individual's personal information, such as that listed above, is eligible for this enhancement. U.S.S.G. § 2B1.1 cmt. n.10(C)(ii)(I).

Although individual conduct can trigger the enhancement, in the case of joint criminal activity -- such as the conspiracy here -- the enhancement may apply based on a co-conspirator's actions if said actions "were (i) within the scope of the jointly undertaken criminal activity, (ii) in furtherance of [said] activity, and (iii) reasonably foreseeable in connection with that criminal activity." U.S.S.G. § 1B1.3(a)(1)(B). In other words, Iwuanyanwu is "not automatically saddled with the full weight of the conspiracy's wrongdoing[,]" but we will find him responsible if his co-conspirators' acts "were reasonably foreseeable by him so long as those acts were committed" in furtherance of the conspiracy and within its scope. United States v. Soto-Villar, 40 F.4th 27, 31 (1st Cir. 2022) (quoting United States v. Sepulveda, 15 F.3d 1161, 1197 (1st Cir. 1993)). The government must establish by a preponderance that the unauthorized use of means of identification was reasonably foreseeable to Iwuanyanwu. Cf. id. We now turn to the issue before us.

"Whether the conduct was reasonably foreseeable to [Iwuanyanwu] is a fact-bound determination that we review for clear error." United States v. Sandoval, 6 F.4th 63, 106 (1st Cir. 2021). Here, the district court found that, based on the record and what was said at the sentencing hearing, the misuse was reasonably foreseeable to Iwuanyanwu. Thus, we will only find clear error if "on the whole of the record, we form a strong, unyielding belief that a mistake has been made." United States v. Teixeira, 62 F.4th 10, 24 (1st Cir. 2023) (quoting United States v. Franklin, 51 F.4th 391, 399 (1st Cir. 2022)).

Before us, Iwuanyanwu argues that he could not have foreseen that a co-conspirator would have fraudulently used S.P.'s identity to open an account in S.P.'s name because he "had limited involvement in the conspiracy" and the scheme's modus operandi was that conspirators would open bank accounts "with their own identities." Moreover, Iwuanyanwu asserts that he played a "middleman role" in the scheme. We are unpersuaded. The record establishes that Iwuanyanwu was not a passive spectator in the conspiracy. He knew the scheme inside and out.

For instance, in a WhatsApp exchange with Motorola 1 regarding the delay in the withdrawal of money from the S.P. account, Iwuanyanwu expressed that in this kind of "business[,] sometimes things like this happen." He expressed confidence that the money was going to be withdrawn soon and advised Motorola 1 to

"relax," "be positive," and not worry. The reasonable import of Iwuanyanwu's statements is that he is well-versed in the ups and downs of BEC schemes. Moreover, we must not overlook the fact that Iwuanyanwu coordinated with "specialists" in schemes like the one here, who drove fifteen hours to withdraw money from the S.P. account.[2] Said level of coordination belies his assertion that he had a limited role or was merely a middleman.

Additionally, although he opened two bank accounts using his own name, he did so by falsely listing himself as the owner, the sole account holder, and the only authorized signer of Victim Company 1 and Victim Company 6 respectively. Moreover, he used fraudulent certificates of incorporation to open the bank accounts. Iwuanyanwu had no affiliation with either company. Even assuming arguendo that Iwuanyanwu was not one of the main players in the scheme, his use of fraudulent corporate documents to open bank accounts used to perpetrate the fraud is sufficient to establish that it was reasonably foreseeable to him that the conspiracy could use false identities when opening additional bank accounts in furtherance of the conspiracy.

[2] It is unclear from the record who the so-called "specialists" were and what their expertise was. However, from the conversation between Iwuanyanwu and Motorola 1, we infer that the "specialists" were individuals accustomed to withdrawing large amounts of cash from fraudulent bank accounts that were part of BEC schemes.

Lastly, Iwuanyanwu relies on a Fifth Circuit case to argue that the misuse of a means of identification enhancement was improperly applied. Our reading of that case leads us to the opposite conclusion. In United States v. Jones, the Fifth Circuit held that the district court correctly applied the misuse of a means of identification enhancement, such as here, because Jones, who acted as a runner in a fraudulent check cashing scheme, could reasonably foresee that the photograph that she provided would be used by the scheme operators to create a false identification card containing her photograph but someone else's personal information. 533 F. App'x 448, 459-60 (5th Cir. 2013) (per curiam) (unpublished). As to the six-point enhancement under U.S.S.G. § 2B1.1(b)(2)(C) (for an offense resulting in substantial financial hardship to twenty-five or more victims), the Fifth Circuit determined that the district court erred in applying said enhancement because Jones could not have foreseen that the scheme operators were getting personal information by stealing mail from collection boxes. Id. at 454-55.

Iwuanyanwu posits that, similar to Jones, he had a limited role in a larger conspiracy. He claims that he was unaware of the other methods used by the scheme to open bank accounts, and thus, the enhancement is inapplicable. The district court did not err in rejecting this argument. Iwuanyanwu was actively involved in the discussions regarding the S.P. account. He exchanged

messages via WhatsApp with Motorola 1 and More Blessing when someone who pretended to be S.P. -- possibly another co-conspirator -- called BB&T to inquire about the account given that there was trouble withdrawing money from it. Likewise, Iwuanyanwu would like us to accept that he believed S.P. had opened the bank account himself "even though []Iwuanyanwu and his co-conspirators were using the account without S.P.'s knowledge and for nefarious purposes." Again, such a contention defies reason given that S.P. would have noticed unknown transactions involving large sums of money, coming from international banks, and would have likely flagged this activity to his bank. Certainly, someone in Iwuanyanwu's position would have thought that a co-conspirator had fraudulently opened the account in S.P.'s name or that S.P. was himself a co-conspirator or someone participating in the conspiracy. Furthermore, as discussed supra, Iwuanyanwu himself used fraudulent certificates of incorporation to open bank accounts, undercutting his argument that the use of fraudulent identifying documents to open accounts was not reasonably foreseeable. Last, but not least, Iwuanyanwu fails to explain why misusing corporate documents is different from misusing personal identification information.

The evidence establishes by a preponderance that it was reasonably foreseeable to Iwuanyanwu that his co-conspirators could open a bank account using a fraudulent name to further the

scheme. Given that the district court's "conclusions were properly rooted in the evidence and its inferences founded in logical reasoning," Sandoval, 6 F.4th at 106 (quoting United States v. Hernández, 218 F.3d 58, 71 (1st Cir. 2000)), the district court did not clearly err in applying the two-point enhancement.

Enhancement for Substantial Financial Hardship

Iwuanyanwu also objects to the two-point enhancement for causing Victim B substantial financial hardship. The conspiracy obtained in a one-month period approximately $6,000 from Victim B, who is disabled, unable to work, and lives with a fixed income of $1,000 per month. The Amended PSR notes that Victim B "received a limited income" and that the amount wired to Iwuanyanwu "was equal to almost six months of income." As a result, Victim B had to take out personal loans shortly thereafter to pay her medical expenses because she had sent to the conspirators all the money that she had available at the time.

The Sentencing Guidelines provide for a two-point enhancement when the offense "resulted in substantial financial hardship to one or more victims." U.S.S.G. § 2B1.1(b)(2)(A)(iii). The commentary thereto provides that, when considering said enhancement, the district court

> shall consider, among other factors, whether the offense resulted in the victim[:]
>
> (i) becoming insolvent;

> (ii) filing for bankruptcy . . .;
>
> (iii) suffering substantial loss of a retirement, education, or other savings or investment fund;
>
> (iv) making substantial changes to his or her employment, such as postponing his or her retirement plans;
>
> (v) making substantial changes to his or her living arrangements, such as relocating to a less expensive home; and
>
> (vi) suffering substantial harm to his or her ability to obtain credit.

Id. cmt. n.4(F). We are mindful that our inquiry must "focus on the victim['s] individual circumstances," "plac[ing] greater emphasis on the extent of harm that [a] particular victim[] suffer[s]." United States v. George, 949 F.3d 1181, 1185 (9th Cir. 2020) (quoting Sentencing Guidelines for Unites States Courts, 80 Fed. Reg. 25,782-01, 25,791 (May 5, 2015)). We review the factual findings underlying the sentencing enhancement for clear error. See Kitts, 27 F.4th at 789.

Iwuanyanwu challenges the finding that Victim B suffered substantial financial hardship because the loans, which were used to pay medical expenses that Victim B incurred, were taken out after the wire transfers. The record supports a finding that the loans were a direct consequence of the scheme because, if Victim B had not been induced to send the wire transfers, she would have had the means to cover her medical bills. Her loss of savings

"inescapably constitutes substantial financial hardship within the ambit of the [G]uidelines." Id. at 790.

Next, Iwuanyanwu contends that the money Victim B transferred was some "extra" money that she had available. However, the record plainly shows how little "extra" money Victim B had after meeting life's basic necessities. Few other substantial life changes could have occurred as a result of her loss because she could not work and already resided with her daughter. Lastly, Iwuanyanwu argues that Victim B visited a local casino frequently, refuting her financial hardship claim. We reject this argument given that the repeat nature of her visits to the casino appears to be incentivized by vouchers sent by the casino, which were valid only for specific periods of time. Because we cannot say that the district court clearly erred in finding that Victim B suffered substantial financial hardship, we find no abuse of discretion in the district court's application of said sentencing enhancement.

Affirmed.