PUBLISHED

UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

No. 22-4261

UNITED STATES OF AMERICA,

Plaintiff − Appellee,

v.

EUNICE BISONG NKONGHO,

Defendant – Appellant.

Appeal from the United States District Court for the District of Maryland, at Greenbelt. George Jarrod Hazel, District Judge. (8:21−cr−00396−GJH−1)

Argued: December 6, 2023 Decided: July 10, 2024

Before DIAZ, Chief Judge, KING and RUSHING, Circuit Judges.

Affirmed by published opinion. Chief Judge Diaz wrote the opinion in which Judge King and Judge Rushing joined.

ARGUED: Megan Elizabeth Coleman, MARCUSBONSIB, LLC, Greenbelt, Maryland, for Appellant. Adam Kenneth Ake, OFFICE OF THE UNITED STATES ATTORNEY, Greenbelt, Maryland, for Appellee. **ON BRIEF:** Erek L. Barron, United States Attorney, Baltimore, Maryland, Joseph R. Baldwin, Assistant United States Attorney, OFFICE OF THE UNITED STATES ATTORNEY, Greenbelt, Maryland, for Appellee.

DIAZ, Chief Judge:

While Eunice Nkongho was under investigation for her role in a munitions export and money laundering conspiracy, federal agents stopped her at the airport and seized her electronic devices. Nine days later, they obtained a warrant to search the contents of her phone. That search unearthed hundreds of inculpatory text messages between Nkongho and her coconspirators.

Nkongho was eventually charged with money laundering and conspiracy to launder money. She moved to suppress evidence from her phone, which the district court denied. At trial, the government relied heavily on her text messages and call history. A jury convicted Nkongho of both counts, and the district court sentenced her to twenty-four months' imprisonment and three years' supervised release.

On appeal, Nkongho challenges the denial of her motion to suppress. She also argues that the district court erred in calculating her sentence. Finding no error on either front, we affirm Nkongho's convictions and sentence.

I.

A.

In 2016, the Department of Homeland Security uncovered a fraud scheme where the conspirators obtained millions of dollars of military equipment, Apple devices, and LG televisions by posing as a United States Navy officer.

During the Department's investigation, a defense contractor reported to Homeland Security Investigations agent Austin Merker that he had sold "highly sensitive

communications interception equipment" to a "Daniel Drunz," *see* J.A. 614, and he had yet to receive any payment. "Drunz" told the contractor that he worked for the United States Navy, and even emailed the contractor from what looked like a U.S. government email address. Under their contract, the contractor sent military equipment worth $3.2 million to a storage location in Chantilly, Virginia.

Merker later determined that the Navy had never employed anyone named Daniel Drunz, and that it knew nothing about the contract. Working in tandem with the Naval Criminal Investigative Service, he learned that "Drunz" had contracted with a second supplier through the same fake government email address. That company shipped around 2,000 LG televisions to the same storage location in Chantilly.

Law enforcement identified two people involved in the scheme, Khalid Razaq and Janet Sturmer, and obtained search warrants for their homes and other storage locations in Virginia. They found stolen LG televisions at each of the storage locations. And in Sturmer's home, they located military equipment sent by the defense contractor.

Both Razaq and Sturmer agreed to speak with law enforcement. Over the course of several interviews in February 2017, Razaq shared that he met Peter Unakalu, the scheme's mastermind, in prison. Unakalu had been deported and was now living in Nigeria, but his wife, Eunice Nkongho, lived in California with their children.

Several months earlier, Unakalu contacted Razaq with an idea for a new scheme. Unakalu told Razaq that he and "Mayor," his "boss," J.A. 615, had a way to fraudulently obtain Apple devices, including iPads and iPhones. But because Unakalu and Mayor were both in Nigeria, they needed Razaq to receive the devices and to store them before

distributing them. Razaq agreed to help, and he and Sturmer received several shipments of the stolen goods over the next few months, including Apple devices, televisions, and military equipment.

After receiving the goods, Razaq coordinated their sale to various buyers in California. Razaq would first ship the goods either to himself or to another coconspirator. He would then work with another coconspirator to deliver them to the buyers. Once the buyers received and paid for the goods, Razaq would distribute the cash proceeds among the scheme's conspirators.

Because Unakalu and Mayor were living abroad, Unakalu instructed Razaq to give their shares of the proceeds to Nkongho, who "handle[d] the money for the organization." J.A. 617. Razaq told law enforcement that he met Nkongho twice, and that he personally gave her more than $200,000 in proceeds from the scheme for Unakalu and Mayor.

After Merker interviewed Razaq, the Department decided to "let the scheme continue," hoping to catch more conspirators. J.A. 518. Around late February, Merker and other agents traveled to California to observe Razaq meet with another coconspirator, Brandon Ross, who gave Razaq a grocery bag filled with $108,000 in proceeds from the scheme.

During that trip, the agents also learned that Unakalu and Razaq planned to move some of the remaining military equipment to Mexico, where the other equipment was stored. The export of such equipment is controlled under federal law. *See* 22 U.S.C. § 2778; 22 C.F.R. § 120 *et seq.*

B.

Merker learned that Nkongho planned to travel to Cuba in March, and that Unakalu planned to travel to Cuba around the same time. Merker asked Customs and Border Protection agents to stop and search Nkongho at the airport before she boarded her flight to Cuba. He also asked them to interview her and to look for "bulk cash and military equipment," since he knew that some of the equipment was outstanding. J.A. 521.

Agents stopped Nkongho traveling with her two children at the Miami International Airport on March 11. Nkongho told the agents that she was meeting Unakalu in Cuba. They asked Nkongho if she was traveling with cash, and she told them that she had about $5,000 with her. The officers searched her purse and discovered around $8,500. They didn't find any military equipment in her luggage. After the search, the agents let Nkongho and her children go, and they traveled to Cuba to meet Unakalu.

On March 17, while Nkongho and her children were still in Cuba, Merker asked Customs and Border Protection agents to seize any electronic devices in Nkongho's possession when she arrived back at the Miami airport. Three days later, on March 20, the agents again stopped Nkongho and her children at the airport. They seized four cell phones and two laptops but didn't arrest Nkongho. They then transferred the devices to Homeland Security Investigations agents to conduct a forensic search.

Because the Homeland Security Investigations agents didn't know whether they needed a warrant to search the devices, they contacted the local U.S. Attorney's Office and their agency's internal legal department for advice. Despite disagreement between the U.S. Attorney's Office and the agency's legal department about needing a warrant, Merker

applied for one on March 29, 2017, nine days after the devices were seized. He received the warrant that day. On April 6 and 7, 2017, agents searched the devices and uncovered incriminating communications between Nkongho, Razaq, Unakalu, and another coconspirator on Nkongho's cell phone.

In the meantime, Nkongho retained an attorney, who reached out to law enforcement to request the return of her devices. Nkongho also directly contacted Homeland Security Investigations about her devices. The agency returned the devices to Nkongho on or around May 9, 2017.

C.

Nkongho and seven coconspirators were charged in a sixteen-count indictment in connection with the scheme. Law enforcement arrested Nkongho at her home. Immediately after her arrest, Nkongho was given *Miranda* warnings and interviewed by law enforcement.

Nkongho later moved to suppress evidence taken from her cell phone, arguing that agents needed a warrant to seize her devices. She also argued that the agents' nine-day delay in seeking a warrant to search her devices was constitutionally impermissible. The district court held a suppression hearing, at which Merker and another federal agent testified.

The district court denied Nkongho's motion to suppress. *United States v. Nkongho*, No. 18-cr-0468, 2021 WL 4421883, at *10 (D. Md. Sept. 27, 2021). The court held that the March 20 seizure of Nkongho's devices fell within the border search exception so that no warrant was required. *Id.* at *4–5. According to the court, the seizure satisfied the

exception's requirement of individualized suspicion of a crime with "a nexus to the sovereign interests underlying the border search exception." *Id.* The court found such a nexus existed because the scheme involved "the theft of military equipment, the transfer of that equipment across international borders, coordination with a co-conspirator located outside of the U.S., and the transfer of proceeds from the illegal sale of the stolen equipment to that co-conspirator." *Id.* at *5.

The court also rejected Nkongho's challenge based on the delay in seeking a search warrant. It found the agents' justification for the delay—that they needed to evaluate "whether a warrant was necessary for the search,"—was "lacking." *Id.* at *6. But it emphasized the government's "heightened interest" in the devices, and it held that the delay wasn't unreasonable. *Id.*[1]

D.

Nkongho also moved to dismiss her indictment based on the government's violation of her Speedy Trial Act rights. In response, the government filed a new indictment against Nkongho. It charged her with one count of conspiracy to launder money, in violation of 18 U.S.C. § 1956(h); and one count of money laundering, in violation of 18 U.S.C. §§ 1956(a)(1)(A)(i) and (B)(i), and 18 U.S.C. § 2. The next day, the district court granted Nkongho's motion to dismiss her original indictment.

[1] The district court also rejected Nkongho's challenges to the March 11 search of her purse and luggage, *id.* at *3, and to the admission of her post-arrest statements, *id.* at *8–9. Nkongho hasn't pursued these claims on appeal.

The case proceeded to trial. At trial, the government introduced several text messages and call records between Nkongho and other coconspirators. It also introduced evidence of Nkongho's banking transactions, which showed a series of deposits she made across different accounts, including Razaq and Ross's accounts, between September 2016 and March 2017.

Several witnesses, including Razaq and another coconspirator, testified about Nkongho's role in the scheme. And the government played excerpts from Nkongho's post-arrest video interview. Nkongho didn't testify.

The jury returned a guilty verdict on both counts.

E.

Before sentencing, Nkongho's probation officer submitted a presentence report. The report calculated Nkongho's total offense level as 28, with a criminal history category of I. Under that calculation, Nkongho's guidelines range was 78 to 97 months' imprisonment, followed by 1 to 3 years' supervised release.

In calculating Nkongho's total offense level, the report first discussed the base level for her offense. Under guideline 2S1.1, the base offense level for laundering of money instruments is the level of "the underlying offense from which the laundered funds were derived," so long as the defendant may be held accountable for the underlying offense and "the offense level for that offense can be determined." U.S.S.G. § 2S1.1(a)(1). The report determined that the underlying offense was wire fraud, which has a base offense level of 6. U.S.S.G. § 2B1.1(a)(2).

On top of the base offense level, the guideline for wire fraud authorizes an enhancement in the offense level based on the loss amount. The report determined that the loss amount from the scheme exceeded $3.5 million, but was less than $9.5 million, so it recommended a corresponding 18-level enhancement. *See* U.S.S.G. § 2B1.1(b)(1)(J).

The report recommended two other enhancements. First, a two-level increase because the offense "resulted in substantial financial hardship to one or more victims." U.S.S.G. § 2B1.1(b)(2)(A)(iii). And second, a two-level increase because "a substantial part of a fraudulent scheme was committed from outside the United States." U.S.S.G. § 2B1.1(b)(10)(B).

Nkongho objected to the offense level calculation. She claimed that because she didn't commit wire fraud, the report erred by using that as the underlying offense for the calculation of the base offense level. She also claimed that the report erred in attributing the fraud conspiracy's entire loss amount to her. And she argued that she was entitled to a reduction for her role in the conspiracy, because her participation in the conspiracy was "minimal." U.S.S.G. § 3B1.2(a). The government had no objections to the report, and the probation officer declined to amend it.

Nkongho renewed her objections at sentencing. But the district court agreed with the government that the proper offense level was 28. It found that the government had proven Nkongho's specific intent to promote the ongoing fraud scheme and receipt of stolen goods, so it could use the fraud guideline to calculate her base offense level, and that at least $4.4 million in losses was reasonably foreseeable to her. It also declined to grant the role reduction.

But after considering the sentencing factors under 18 U.S.C. § 3553(a), the district court granted Nkongho a substantial downward variance, sentencing her to 24 months' imprisonment followed by 3 years' supervised release as to each count, to run concurrently. It also ordered Nkongho to pay $399,780 in restitution and a $100 special assessment on each count.

This appeal followed.

II.

Nkongho challenges both the denial of her motion to suppress and the calculation of her sentence. She argues that the seizure of her devices went beyond the border search exception and, in the alternative, that the agents' nine-day delay in seeking the search warrant was unreasonable. As to her sentence, she argues that the district court clearly erred when it attributed more than $4.4 million in losses from the fraud conspiracies to her. She also argues that the district court clearly erred when it declined to impose a role reduction.

We review each contention in turn.

A.

We begin with Nkongho's motion to suppress. When the district court denies a motion to suppress, we review its legal conclusions de novo and factual findings for clear error. *United States v. Green*, 740 F.3d 275, 277 (4th Cir. 2014). We consider the evidence in the light most favorable to the government, the prevailing party below. *Id.*

1.

The Fourth Amendment safeguards "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV. That means that an officer must generally obtain a warrant, supported by probable cause, to search or seize someone's person or property. *Riley v. California*, 573 U.S. 373, 382 (2014). But "[t]his usual requirement . . . is subject to a number of exceptions." *Birchfield v. North Dakota*, 579 U.S. 438, 456 (2016).

The border search exception is one such example. Acknowledging our nation's inherent sovereign interests in "protecting . . . territorial integrity," *United States v. Flores-Montano*, 541 U.S. 149, 153 (2004), and "prevent[ing] the introduction of contraband," *United States v. Montoya de Hernandez*, 473 U.S. 531, 537 (1985), the Supreme Court has long held that border agents need no warrant, nor any individualized suspicion, to conduct "routine searches of the persons and effects of entrants," *Montoya de Hernandez*, 473 U.S. at 538. And agents may conduct warrantless nonroutine searches if they have reasonable suspicion that the entrant is engaged in contraband smuggling. *See id.* at 541, 542 (holding that agents could detain a traveler for sixteen hours to see if she had smuggled narcotics in her digestive system).

The ubiquity of smartphones has broadened the potential scope of this exception. Now, when travelers enter the United States, they carry with them not only a suitcase, but also "the sum of [their] private li[ves]." *Riley*, 573 U.S. at 394. A traveler's phone will contain "unusually sensitive data regarding one's relationships, personal interests and preferences, prior internet searches, location history, and much more." *United States v.*

Aigbekaen, 943 F.3d 713, 723 (4th Cir. 2019). And through a forensic search—"a powerful tool capable of not only viewing data that a user has intentionally saved on a digital device, but also unlocking password-protected files, restoring deleted material, and retrieving images viewed on websites," *id.* at 718 n.2 (cleaned up)—border agents may access an "unparalleled breadth of private information," *United States v. Kolsuz*, 890 F.3d 113, 143–44 (4th Cir. 2018).

Yet despite the privacy interests at stake, forensic searches conducted under the border search exception are critical for preventing cross-border crime and the importation of contraband. For instance, a phone may contain digital contraband, such as child pornography. *See United States v. Cano*, 934 F.3d 1002, 1013–14 (9th Cir. 2019). Or it may contain evidence of ongoing transnational criminal activity, *see Kolsuz*, 890 F.3d at 143–44, such as communications between conspirators.

We've recognized that "[t]he justification behind the border search exception is broad enough to accommodate not only the direct interception of contraband as it crosses the border, but also the prevention and disruption of ongoing efforts to export contraband illegally." *Id.* Other circuits have endorsed this rule. *See Alasaad v. Mayorkas*, 988 F.3d 8, 20 (1st Cir. 2021) ("[T]he border search exception is not limited to searches for contraband itself rather than evidence of contraband or a border-related crime."); *United States v. Gurr*, 471 F.3d 144, 149 (D.C. Cir. 2006) (holding that in the context of border searches, the "distinction . . . between contraband and documentary evidence of a crime is

without legal basis"); *United States v. Xiang*, 67 F.4th 895, 900 (8th Cir. 2023) (rejecting argument that the Fourth Amendment doesn't permit border searches for evidence).[2]

In short, the government's interests at the border are paramount, and forensically searching a traveler's electronic devices may be vital to promoting those interests.

Nonetheless, given the sheer mass of intimate information available in a forensic search, the government may rely on the border search exception to conduct such a search in only limited circumstances. Before we will countenance such a search, the government must show that it "ha[d] individualized suspicion of an offense that bears some nexus to the border search exception's purposes of protecting national security, collecting duties, blocking the entry of unwanted persons, or disrupting efforts to export or import contraband." *Aigbekaen*, 943 F.3d at 721.

Admittedly, we've established this rule for *searches* of devices, not *seizures* of them. And here, though agents *seized* Nkongho's devices at the airport citing the border search exception, they didn't forensically *search* her devices until they obtained a warrant.

But we think the same rule should apply. After all, a forensic search of an electronic device necessarily involves seizing it, as the search can take weeks to complete. *See United States v. Saboonchi*, 990 F. Supp. 2d 536, 569 (D. Md. 2014) (noting that a forensic search

[2] The Ninth Circuit has adopted the opposite rule. In *United States v. Cano*, it disagreed with *Kolsuz* and held that "cell phone searches at the border, whether manual or forensic, must be limited in scope to a search for digital contraband." 934 F.3d 1002, 1007, 1017–18 (9th Cir. 2019). Nkongho argues that *Kolsuz* was wrongly decided. Of course, this panel has no power to overrule *Kolsuz*. *See United States v. Williams*, 808 F.3d 253, 261 (4th Cir. 2015) ("In this circuit, we are bound by the basic principle that one panel cannot overrule a decision issued by another panel." (cleaned up)).

may deprive the cell phone's owner of her device for days or weeks). A traveler has a strong possessory interest in her phone and other electronic devices, *cf. United States v. Pratt*, 915 F.3d 266, 272 (4th Cir. 2019), though that interest may be tempered while she's in government custody, *see Kolsuz*, 890 F.3d at 141. But even if she is detained, she still has a strong privacy interest in those devices. *Cf. Riley*, 573 U.S. at 398.

We recognize that a traveler has a diminished expectation of privacy at the border. *See Flores-Montano*, 541 U.S. at 154. Yet extending the individualized suspicion and transnational nexus requirements to the nonroutine seizure of a phone for the purpose of a forensic search protects the traveler's interests and keeps the seizure tethered to the rationale behind the border exception.

Here, though, the government satisfies those requirements.

First, federal agents had probable cause to believe that Nkongho was part of a munitions export conspiracy. As the district court correctly noted, neither *Kolsuz* nor *Aigbekaen* decided whether reasonable suspicion is enough to justify a forensic search or whether probable cause is required. *See Kolsuz*, 890 F.3d at 137, 147 (applying good-faith exception and noting that it "need not resolve" the appropriate level of suspicion); *Aigbekaen*, 943 F.3d at 723 (declining to determine "what quantum of individualized suspicion" is needed "to justify a warrantless forensic search of a device at the border").

Absent such guidance, the district court applied a reasonable suspicion standard. *See Nkongho*, 2021 WL 4421883, at *4 n.3. As we explain, we too need not decide whether that ruling was correct.

Nkongho concedes that agents had probable cause to seize her devices on March 20. But she claims that they had probable cause for only *domestic* offenses—wire fraud and receipt of stolen property—which aren't tethered enough to the exception's justifications of stopping *transnational* crime. *See Aigbekaen*, 943 F.3d at 721 (holding that exception didn't apply to a traveler who was suspected of inter*state* sex trafficking that lacked "any . . . transnational component").

Nkongho is wrong. At the time of the seizure, agents had probable cause to believe that Nkongho was part of an international munitions export scheme. Indeed, nine days after agents seized Nkongho's devices, a magistrate judge found probable cause that she was part of a conspiracy to violate the Arms Export Control Act, 22 U.S.C. § 2778 *et seq.*, and issued a warrant to conduct the forensic search.

That the magistrate judge also found probable cause for five other offenses is of no moment. It's well-established that a single conspiracy may have multiple objects. *See United States v. Young*, 989 F.3d 253, 263 (4th Cir. 2021). So we need not consider whether the conspirators' fraud and theft offenses also had a sufficient transnational component to justify the seizure.

In *Kolsuz*, we upheld the forensic search of the defendant's phone when border agents suspected him of violating weapons export laws. 890 F.3d at 144. As we remarked, "That is a transnational offense that goes to the heart of the border search exception, which rests in part on the sovereign interest of protecting and monitoring exports from the country." *Id.* at 143 (cleaned up). So too here.

To be sure, the facts of *Kolsuz* aren't identical. Unlike Nkongho, agents apprehended Kolsuz while he was violating weapons export laws. *Id.* Agents searched Kolsuz's luggage at the airport as he was attempting to leave the United States, and they discovered firearm parts that Kolsuz couldn't export without a license. *Id.* at 139. And Kolsuz admitted that he didn't have a license. *Id.* So agents arrested him, seized his phone, and then forensically searched it without a warrant. *Id.*

But we disagree that Nkongho needed to be caught in the act when agents seized her phone for the border search exception to apply. As the magistrate judge found, agents had probable cause to believe that her devices would contain evidence of a conspiracy to violate munitions export laws. The agents knew that Razaq and Unakalu planned to ship military equipment to Mexico, in violation of federal export regulations. And they were aware of Nkongho's role in the conspiracy; Razaq had told agents that Nkongho "handles the money for the[ir] organization," J.A. 617, and that he had personally given Nkongho proceeds from the stolen goods to give to her husband, the scheme's mastermind.

The agents' interactions with Nkongho at the airport only bolstered the probable cause for the conspiracy. Nkongho told agents that she planned to meet her husband in Cuba. She then told them that she had $5,000 in her purse, but a search revealed $8,500. Together with the amount of bulk cash, Nkongho's misrepresentation reasonably strengthened the officers' suspicions.

And even though the agents didn't find the stolen military equipment in Nkongho's luggage, they knew that she was part of the conspiracy. Their belief that "there may have been other communications between her and her husband about the fraud scheme or the

movement of money" on her devices, *see* J.A. 522, was therefore supported by probable cause.

The government gives us a second (though unnecessary) ground to affirm the district court. It argues that it had probable cause to suspect that Nkongho's devices would contain digital contraband. It claims that because the stolen military equipment was controlled for export, it would be illegal to photograph. Thus, it argues, any photograph of the equipment on Nkongho's devices would be digital contraband, and the agents had probable cause to seize and search her devices to find this contraband.

But because the government didn't make that argument in the district court, it's forfeited, and we decline to consider it. *See Williams v. Pro. Transp. Inc.*, 294 F.3d 607, 614 (4th Cir. 2002). In any event, it wouldn't impact our holding.

To reiterate, the government needn't show there was digital contraband on the device. *Kolsuz* holds that the border search exception extends to both contraband and other evidence of a crime. 890 F.3d at 143–44. Because the agents reasonably suspected that the devices would contain evidence of an international fraud scheme, involving sensitive military equipment, we affirm the lawfulness of the seizure.[3]

[3] The agents seized Nkongho's devices before our decisions in *Kolsuz* and *Aigbekaen*. As we said in *Kolsuz*, we think it reasonable for the agents who seized Nkongho's devices "to rely on the established and uniform body of precedent allowing warrantless border searches of digital devices that are based on at least reasonable suspicion." 890 F.3d at 148. Though we affirm the seizure of Nkongho's devices on the merits, we think the good-faith exception also applies on these facts. *See also Aigbekaen*, 943 F.3d at 725 (applying good-faith exception to pre-*Kolsuz* border search).

2.

Nkongho next argues that even if the government could have seized her devices under the border search exception, it did so unreasonably by waiting nine days to seek a search warrant. We aren't convinced that this delay was unreasonable.

To be sure, "a seizure reasonable at its inception must remain reasonable in scope and duration to satisfy the Fourth Amendment." *Kolsuz*, 890 F.3d at 141 (citing *Montoya de Hernandez*, 473 U.S. at 541–52). So an unreasonable delay in completing a search will violate the Fourth Amendment. *Pratt*, 915 F.3d at 272–73.

In *Pratt*, for example, we held that the government's thirty-one-day delay in applying for a warrant to search the defendant's phone was unreasonable. 915 F.3d at 273. In doing so, we compared the defendant's possessory interest in his phone with the government's interest in searching for evidence. *Id.* at 271. Because the defendant retained a strong possessory interest in the phone, and because the government's long delay was unjustified, we held that the district court should have granted his motion to suppress. *Id.* at 273.

Pratt didn't involve a border search, but it logically extends to this context. We explicitly left open this possibility in *Kolsuz*. *See* 890 F.3d at 141. There, we recognized that the defendant was in custody while the government completed its forensic search, so we declined to "address whether and under what circumstances an extended confiscation of a traveler's phone—quite apart from any search undertaken—might constitute an unreasonable seizure of property for Fourth Amendment purposes." *Id.* Because Nkongho

wasn't detained while the government searched her devices, that question is before us today.

We agree with Nkongho that an unreasonably delayed forensic search of electronic devices at the border *can* render their continued seizure impermissible. But on these facts, we can't say that the government's nine-day delay did so.

As in *Pratt*, Nkongho's possessory interest in her devices was no doubt high. She wasn't detained. Nor did she consent to the seizure or willingly share any of the contents of her devices with the agents. *See Pratt*, 915 F.3d at 271–72. And both she and her attorney contacted law enforcement to request that they be returned. *See United States v. Burgard*, 675 F.3d 1029, 1033 (7th Cir. 2012) (recognizing that checking on the status of the search and requesting return of the seized items can evidence a possessory interest).

But we must balance Nkongho's strong possessory interest with the length of the delay and the government's justifications for it.

Here, the nine-day delay was relatively short, and courts have upheld delays of similar length. *See id.* at 1033–34 (six days); *United States v. Martin*, 157 F.3d 46, 54 (2d Cir. 1998) (eleven days). So this factor favors the government.

The government's justification needs more discussion. Nkongho argues that the government's purported rationale—that it needed time to research the need for the warrant—is like the explanation we rejected in *Pratt*. There, the officer delayed the search by thirty-one days to determine *where* to seek the warrant, either in North Carolina or South Carolina. 915 F.3d at 272. We found that the government failed to "exercise diligence" and hadn't provided a "persuasive justification for the delay." *Id.*

Nkongho argues that *United States v. Mitchell*, an Eleventh Circuit decision, is also on point. There, the Eleventh Circuit found the officer's testimony that he didn't think the warrant was urgent to be insufficient. 565 F.3d 1347, 1351 (11th Cir. 2009).

But in both *Pratt* and *Mitchell*, the law was clear that the officers needed a warrant—they just didn't act diligently in seeking one. Here, it wasn't clear whether a warrant was required.

Recall that the agents completed the forensic search in March 2017, before we'd decided either *Kolsuz* or *Aigbekaen*. At the time, the only precedent in our circuit was *Saboonchi*, a district court order that held that officers didn't need a warrant for a forensic search at the border. *See* 990 F. Supp. 2d at 548. In the interim, the Supreme Court invalidated a warrantless search of a phone under the search incident to arrest exception. *See Riley*, 573 U.S. at 386.

So it's understandable why the agents may have had doubts, and why they took the commendable step of consulting legal counsel. If the agents had opted not to get a warrant when they needed one, the district court may have suppressed the evidence from Nkongho's devices, which would have likely been fatal for the prosecution.

Still, Nkongho argues that since the agents decided on March 17 that they would seize her devices upon her return from Cuba, they could have researched the warrant issue before they seized them on March 20. Maybe so, but we don't think the three extra days makes the delay unreasonable. And though we ultimately hold that a warrant wasn't required, we decline to fault the officers for affording Nkongho greater protection than she was due.

B.

Turning to her sentence, Nkongho argues that the district court clearly erred in its calculation of her guidelines level. First, Nkongho contends that the district court erred when it calculated the base offense level for her money laundering conspiracy, as the losses from the fraud conspiracy weren't reasonably foreseeable to her. Second, Nkongho asserts that she met her burden of proving that she was entitled to a two-level reduction, as her participation in the conspiracy was "minor" or "minimal."

We disagree on both counts.

1.

The sentencing guidelines provide two ways to calculate the base offense level for money laundering convictions. U.S.S.G. § 2S1.1(a).

First, under guideline 2S1.1(a)(1), the base offense level may be "[t]he offense level for the underlying offense from which the laundered funds were derived, if . . . the offense level for that offense can be determined. " But subsection (a)(1) applies only to direct money launderers, who either committed the underlying offense or are otherwise accountable for it because they "aided, abetted, counseled, commanded, induced, procured, or willfully caused" it. U.S.S.G. § 1B1.3(a)(1)(A); U.S.S.G. § 2S1.1(a)(1); *see also* U.S.S.G. app. C, amend. 634 (describing the difference between "direct money launderers" under subsection (a)(1) and "third party money launderers" under subsection (a)(2)).

If the defendant didn't commit the underlying offense or isn't otherwise accountable for it, then the court will calculate the base offense level under subsection (a)(2). Under

that subsection, the base offense level is eight plus an enhancement "corresponding to the value of the laundered funds." U.S.S.G. § 2S1.1(a)(2).

The district court calculated Nkongho's base offense level under subsection (a)(1). As to the underlying offense, it found that Nkongho "was aiding and abetting . . . the ongoing fraud scheme, as well as the receipt of stolen goods." J.A. 706.[4] So it calculated her base offense level based on guideline 2B1.1, which establishes the base offense level for fraud offenses and offenses involving stolen property.

Guideline 2B1.1(b)(1) permits a court to increase the base offense level for a fraud offense based on the loss amount, so long as the loss exceeded $6,500. As relevant here, a court may impose an 18-level enhancement if the loss amount falls between $3.5 million and $9.5 million.

Based on Nkongho's participation in the fraud conspiracy, the court attributed more than $4.4 million in losses to her, triggering the 18-level enhancement. Specifically, it adopted the presentence report's loss amount calculation of $1.28 million from the stolen Apple devices and $3.185 million from the LG televisions, for a total of $4.465 million. The court recognized that even if Nkongho wasn't "directly . . . involved" in the theft of those goods, the guidelines permitted it to consider any losses incurred within the scope of the conspiracy that were "reasonably foreseeable" to her. J.A. 706 (quoting U.S.S.G. §

[4] While the presentence report specifies wire fraud as the underlying offense, the district court seemed to identify the wire fraud *conspiracy*. Nkongho doesn't challenge this distinction.

1B1.3(a)(1)(B)). And it found that, based on her involvement in the conspiracy, Nkongho could reasonably foresee the total loss amount from those goods.

Nkongho challenges that determination, claiming that she personally handled only around $400,000 of the conspiracy's proceeds. And she insists that she "never received shipments, transported, sold, or laid eyes on any of the volumes of products." Appellant's Br. at 49.

But our consideration of the district court's loss calculation is limited. While we review the district court's application of the guidelines de novo, *United States v. Catone*, 769 F.3d 866, 875 (4th Cir. 2014), we review its factual findings, including its loss calculation, for clear error, *United States v. Cloud*, 680 F.3d 396, 409 (4th Cir. 2012). And as to the latter, we simply determine "whether the district court's account of the evidence is *plausible* in light of the record viewed in its entirety." *United States v. Wooden*, 887 F.3d 591, 608–09 (4th Cir. 2018) (cleaned up) (emphasis added).

Given the ample evidence of Nkongho's participation in the fraud conspiracy, we don't think the district court clearly erred.

Nkongho knew that Unakalu and Razaq planned to fraudulently obtain both the Apple devices and televisions. When Razaq first gave Nkongho the proceeds from the stolen iPads and iPhones, she asked, "Are these from the Apple products?" J.A. 370–73. A few weeks later, when Razaq gave Nkongho a second payment from the fenced Apple devices, Nkongho told him, "[Unakalu] told me that there is going to be more big orders coming." J.A. 382, 385–87. Later, after the conspirators obtained the LG televisions, Unakalu texted Nkongho that he needed space to store "thousands of goods." J.A. 476.

He also told her that they had received "a lot of product that needs to be shipped immediately." J.A. 475. Nkongho researched potential storage facilities for the goods around the same time.

And Nkongho was in constant communication with her coconspirators—especially Unakalu, her husband and the scheme's mastermind. *See United States v. Otuya*, 720 F.3d 183, 191 (4th Cir. 2013) (finding that loss was reasonably foreseeable to the defendant when "he had a close working connection with the conspirators" who perpetrated the fraud); *cf. United States v. Rivera-Rodriguez*, 318 F.3d 268, 273–75 (1st Cir. 2003) (finding that entire loss amount wasn't attributable to defendant, when defendant didn't know the other participants of the conspiracy or know that they had engaged in money laundering transactions).

Finally, Nkongho played an active role in the fraud conspiracy. She engaged in at least twenty money laundering transactions in furtherance of the scheme, including depositing illicit proceeds in her coconspirators' bank accounts. And Unakalu often directed her to give money to Razaq and two of their other coconspirators. Even if he never told her how much the scheme was pilfering, a reasonable person in her position could have intuited that the losses may have exceeded $4.4 million.

Against this backdrop, we don't think the district court clearly erred in attributing the total loss amount from the fraud conspiracy to Nkongho. The 18-level increase was proper.

2.

Nkongho lastly argues that the district court should have decreased her offense level under guideline 3B1.2(a) based on her limited role in the conspiracy. We review the district court's determination of the defendant's role in the offense for clear error. *United States v. Sayles*, 296 F.3d 219, 224 (4th Cir. 2002).

Under guideline 3B1.2, the court may decrease the offense level by four points if the defendant played a "minimal" role in the offense, or by two points if she played a "minor" role in the offense. *Id.* And it may decrease the guidelines calculations by three levels if her conduct fell in the middle of "minimal" and "minor." *Id.*

The district court declined to grant such a reduction because Nkongho played a "significant role" in the money laundering conspiracy. J.A. 708. The record more than supports that finding.

To reiterate, Nkongho personally handled approximately $400,000 in illicit proceeds and engaged in money laundering transactions in furtherance of the conspiracy for at least seven months. Considering these facts, the district court didn't clearly err when it declined to impose a role reduction.

***

For these reasons, we affirm the district court's judgment.

AFFIRMED