No. _____

IN THE

SUPREME COURT OF THE UNITED STATES

═══════════

JEFFREY LANGFORD,

Petitioner,

- v -

UNITED STATES OF AMERICA,

Respondent.

═══════════

ON PETITION FOR WRIT OF CERTIORARI
TO THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

═══════════

PETITION FOR WRIT OF CERTIORARI

═══════════

STEVEN A. BRODY
State Bar No. 271616
155 N Lake Ave, Ste 800
Pasadena, CA 91101
T: 213-290-5294
F: 213-403-5323
stevebrodylaw@gmail.com
Attorney for Petitioner

Appointed Under the Criminal Justice Act of 1964

QUESTIONS PRESENTED FOR REVIEW

1. Whether the Fourth Amendment permits the government to seize cell phones under a warrant imposing a 120-day search deadline, take no steps to initiate a search for more than 200 days, and obtain an extension of time without disclosing to the magistrate that no review had begun.
2. Whether probable cause exists to search a residence for evidence of identity fraud based on a single, undated use of another person's identifying information on a rental application, where the alleged victim was never contacted and the nexus between the offense and the premises rests solely on generalized training-and-experience testimony.

PARTIES TO THE PROCEEDING

Petitioner is Jeffrey Langford, the defendant/appellant in the proceedings below.

Respondent is the United States of America.

STATEMENT OF RELATED PROCEEDINGS

The proceedings identified below are directly related to the above-captioned case in this Court.

- *United States v. Jeffrey Langford,* No. 23-3681, U.S. Court of Appeals for the Ninth Circuit, affirming sentence and conviction, decided February 23, 2026.
- *United States v. Jeffrey Langford,* No. 2:18-cr-00195-GW-1, U.S. District Court for the Central District of California. Judgment entered November 9, 2023.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Constitutional Provisions

PETITION FOR WRIT OF CERTIORARI

Petitioner Jeffrey Langford respectfully petitions for a writ of certiorari to review the judgment of the United States Court of Appeals for the Ninth Circuit in this case.

OPINION BELOW

On February 23, 2026, the Ninth Circuit Court of Appeals issued an unpublished memorandum disposition affirming the district court's denial of petitioner's suppression motion and petitioner's resulting sentence and conviction. Appendix A.

JURISDICTION

The court of appeals entered its judgment on February 23, 2026. This Court has jurisdiction under 28 U.S.C. § 1254(1) .

CONSTITUTIONAL AND STATUTORY PROVISIONS

The Fourth Amendment to the United States Constitution provides: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."

INTRODUCTION

This case presents two questions about the Fourth Amendment's application to increasingly common law enforcement practices that lack meaningful guidance from this Court.

First, the government seized petitioner's cell phones under a warrant that imposed a 120-day deadline to complete its search. It took no action whatsoever during that period—not even transporting the phones to a forensic laboratory. When the deadline lapsed, the government obtained an extension by citing forensic backlogs and technical difficulties, without disclosing that the phones had not yet been provided to the lab. Both phones were searched within weeks of the extension being granted. The Ninth Circuit found no Fourth Amendment violation and, in the alternative, applied the good-faith exception. This Court has never addressed what obligation of diligence the Fourth Amendment imposes on the government after it seizes a digital device, or what consequences follow when the government obtains a judicial extension based on incomplete disclosures.

Second, the government obtained a warrant to search petitioner's apartment for evidence of identity fraud based on an affidavit alleging a single use of another person's identifying information on an undated rental application. The affidavit did not allege that the victim had been contacted, that he had denied authorizing the use of his information, or that the alleged fraud was part of any continuing scheme. The Ninth Circuit upheld the warrant based largely on the affiant's generalized assertion that identity thieves keep evidence in their homes. Lower courts need guidance on the probable cause standard applicable to discrete, completed fraud offenses—which,

unlike ongoing drug trafficking or possession of contraband, do not give rise to a reasonable inference that evidence will still be on the premises.

STATEMENT OF THE CASE

A. Procedural background.

Petitioner was charged in a First Superseding Indictment on May 7, 2019, in count one with conspiracy to distribute methamphetamine in violation of Title 21 U.S.C. § 846, in count two with possession with intent to distribute methamphetamine in violation of 21 U.S.C. §§ 841(a)(1), (b)(1)(A)(viii), in count three with use of an unauthorized access device in violation of 18 U.S.C. § 1029(a)(2), and in count four with aggravated identity theft in violation of 18 U.S.C. § 1028A(a)(1). 3-ER-401–07.

On August 20, 2021, petitioner filed a motion to suppress evidence seized during the search of his residence, arguing that the warrant application lacked probable cause to believe evidence of fraud would be found on the premises and that the government unreasonably delayed in executing a subsequent "roll-back" warrant for the search of cell phones found during the initial search. 4-ER-432.

On September 20, 2021, the district court held a hearing on the motion to suppress. 2-ER-50–86. In a written order filed the same day, the court denied the motion. 1-ER-7–26; Appendix C.

Pursuant to a plea agreement (2-ER-28–49), petitioner conditionally pleaded guilty to possession with intent to distribute methamphetamine (count two) and aggravated identity theft (count four) as charged in the First Superseding Indictment,

reserving his right to appeal the district court's denial of his suppression motion. CR 154.

According to the facts recited in the plea agreement, petitioner knowingly used the personal identifying information of C.W.—including birthdate, Social Security number, address, and a tax return—without authorization, to fraudulently lease an apartment. The defendant used this information in connection with the felony offense of using unauthorized access devices, in violation of 18 U.S.C. § 1029(a)(2). Petitioner further knowingly possessed with intent to distribute 16.1 kilograms of methamphetamine and 18.09 grams of cocaine. Petitioner knew he possessed at least 500 grams of methamphetamine and intended to distribute both drugs to others. 2-ER-36–38.

On November 9, 2023, the district court sentenced petitioner to 162 months imprisonment, consisting of 138 months on count two and 24 months on count four, to be served consecutively. A period of five years supervised release was imposed to follow custody. 1-ER-2; Appendix B.

Petitioner filed a timely notice of appeal on November 21, 2023. 3-ER-408.

B. Facts relevant to petitioner's motion to suppress evidence.

1. The government applies for a search warrant asserting probable cause to believe that evidence of fraud will be found at petitioner's residence.

On March 12, 2018, the government applied for a warrant authorizing a search of an apartment located on Santee Street in Los Angeles, where petitioner was believed to be residing, on the ground that probable cause existed to believe that

evidence of violations of 18 U.S.C. §§ 1028, 1028A, and 1029 would be found on the premises. 2-ER-131–71.

The application was supported by an affidavit from FBI Agent Kamaeol Wong. Agent Wong stated that petitioner had come to the FBI's attention in the course of an investigation into the death of J.A., a 22-year-old who had died from a fentanyl overdose on August 22, 2016. 2-ER-154–55.

In October 2016, J.A.'s family member provided law enforcement "screenshots of J.A.'s text messages with the apparent supplier of the Fentanyl." Those messages included one from J.A. to the supplier at 3:16 a.m. on the day of J.A.'s death in which J.A. stated, "Call me in the morning. You gave me something by accident." 2-ER-155. Police determined that the recipient phone number belonged to petitioner and that he had been in touch with J.A. "12 times on the day of J.A.'s death." 2-ER-155. The phone number was listed in J.A.'s phone as "Jeff Mitches friend," and was subscribed to the same address listed on petitioner's driver's license. *Id*.

The affiant further stated that "[a] confidential source [] later told investigators that s/he had purchased cocaine from [petitioner] approximately 5-10 times in the past, and that s/he gave [petitioner's] phone number to J.A. for the purpose of purchasing cocaine." 2-ER-155. The affiant did not state when the source provided this information, nor when the alleged past purchases of cocaine had taken place. *Id*.

In November 2017, fifteen months after the death of J.A., another confidential source (who had previously been terminated from the DEA for extorting money from

a DEA target and his family) stated that petitioner was residing at the Santee apartment. 2-ER-155–56. However, the warrant application gave no indication of when petitioner had first begun residing at the apartment.

Agents saw petitioner around the premises in November 2017 and in January 2018. In January 2018, an agent showed the Santee apartment general manager petitioner's driver license photograph. 2-ER-156. The general manager told agents that the person in the photograph resided at the Santee apartment but said that his name was C.W., not Langford. *Id*. The general manager then showed agents the rental application for the apartment. *Id*.

The application fee had been paid with a credit card in petitioner's name, but the biographical information—including the date of birth, social security number, address, and criminal history—was not petitioner's. 2-ER-156. The warrant application did not identify the person whose information matched those data. However, a tax return provided with the application for proof of income belonged to C.W. *Id*. The affiant provided no facts regarding who had received the application—whether it was the general manager or some other party—nor when the application was made.

An agent retrieved a copy of the Massachusetts driver's license for C.W., which listed the date of birth and address that petitioner had provided on the rental application. 2-ER-156–57. Two months later, in March 2018, the general manager told agents that Defendant still resided at the Santee apartment. 2-ER-156. The affiant did not say whether police had ever contacted or interviewed C.W.

Agent Wong stated in the affidavit that, based on his training and experience, "drug traffickers often use false identities to facilitate and conceal their crimes," including their own identity and the locations at which transactions take place. 2-ER-157. That may include "vehicles, properties, telephones, utilities, and other items purchased in the names of others, and through the use of stolen identities" to conceal their crimes. *Id*. Wong stated that "[i]dentity thieves will . . . steal and maintain several identities at once to facilitate their crimes, and keep evidence of their crimes in their residences." *Id*. Such individuals "heavily utilize cellular telephones and other electronic devices to communicate with one another and to commit and conceal their crimes," and these devices often contain evidence of the crimes. *Id*.

The magistrate issued the warrant ("March 12 Warrant"), authorizing the search of the Santee apartment and the seizure of the items listed in the application, consisting of "evidence, fruits, and instrumentalities of identity theft and access device fraud in violation of 18 U.S.C. §§ 1028, 1028A, and 1029 ('Subject Offenses')." 2-ER-134.

2. The execution of the warrant results in the seizure of narcotics and digital devices.

Agents executed the search on March 19, 2018. Petitioner and another man, D.F., were in the apartment. Agents found approximately 25 to 30 pounds of methamphetamine, a half ounce of cocaine, and a pound of marijuana, in various packaging. 2-ER-196. During the execution of the warrant, another individual, Brandon Thompson arrived carrying packages like those containing the drugs found in the apartment. Thompson's phones were seized. Agents also found and seized two

cell phones belonging to petitioner. 2-ER-197. One of petitioner's phones was unlocked and did not need a passcode or other input to access the device. 2-ER-269. Agents searched through that phone and found text messages between petitioner and Thompson discussing drug sales. 2-ER-197, 269. Petitioner's other phone was locked. 2-ER-269, 278.

3. The government obtains "rollback" warrants to search seized digital devices but does not initiate a search of petitioner's phones before the 120-day window to do so has closed.

The same day the warrant was executed, agents applied for "rollback warrants" to search the seized digital devices of both petitioner and Thompson. 2-ER-182. The warrant prohibited the government from searching the devices beyond 120 days of the execution of the original warrant. 2-ER-190. However, by September 28, 2018, petitioner's digital devices had not yet been searched, causing the government to apply ex parte for an extension of time. 2-ER-266–71. In fact, by the time the government applied for the extension, the phones had not yet even been sent to the forensics laboratory. 1-ER-24; 2-ER-276, 278. The government supported its extension application on the ground that "the forensic review of digital devices is time consuming" and that "both the FBI and the DEA have an extensive backlog of devices to review in criminal cases." 2-ER-270. The application made no mention of the fact that the government had not yet even transported the phones to the laboratory to be analyzed.

The government finally transported the phones to the forensic laboratory in October, more than 200 days after the March 19, 2018 warrant had issued. 2-ER-276,

278. Agents completed a forensic search of one of the phones on October 5; the computer forensic laboratory unlocked the other phone on November 10, and the agents completed the search of that phone on November 28, 2018. 2-ER-276, 278.

C. The Ninth Circuit's Decision

On February 23, 2026, a three-judge panel (Graber, Bress, and Johnstone, Circuit Judges) affirmed in an unpublished memorandum. App. A. The panel held that the March 12 warrant was supported by probable cause based on petitioner's use of C.W.'s identifying information on the rental application and the affiant's training-and-experience testimony that identity thieves keep evidence in their residences. App. A at 2. As to the March 19 warrant, the panel held that the seven-month delay between seizure and search of petitioner's phones did not violate the Fourth Amendment, crediting the government's stated justifications for the delay and finding that the warrant did not require the extension request to be filed within the original 120-day period. App. A at 3. In the alternative, the panel held that the good-faith exception applied because petitioner offered no evidence that the government deliberately tarried or misled the court, and because the agents reasonably relied on the magistrate judge's extension order and the judgment of the government's attorneys. App. A at 3–4.

REASONS FOR GRANTING THE PETITION

I. The Court Should Grant Certiorari to Clarify for Lower Courts the Method of Evaluating the Reasonableness of Post-Seizure Delay in Reviewing Digital-Device Contents Under the Fourth Amendment.

A. Lower courts lack meaningful guidance on a question of growing national significance.

This Court has never squarely addressed the standard governing the reasonableness of delays between the seizure of a digital device and the government's initiation of a search of its contents. Lower courts have been left to navigate this increasingly important question with virtually no guidance.

While courts have recognized that digital device searches may involve technical delays, they have also distinguished between delays in completing a search and delays in initiating one. In *United States v. Metter*, 860 F. Supp. 2d 205 (E.D.N.Y. 2012), the court addressed the question of how long the government could delay before commencing a search of seized data. There, the government imaged the defendant's hard drives but failed to begin reviewing the data for more than fifteen months. *Id.* at 210–11.

Though "under current law there is no established upper limit as to when the government must review seized electronic data to determine whether the evidence seized falls within the scope of a warrant," *Metter* nevertheless found the delay unreasonable under the Fourth Amendment because the government did not even begin its execution of the warrant until many months after the seizure of the hard drives:

> The parties have not provided the Court with any authority, nor has the Court found any, indicating that the government may seize and image electronic data and then retain that data with no plans whatsoever to *begin* review of that data to determine whether any irrelevant, personal information was improperly seized. The government's blatant disregard for its responsibility in this case is unacceptable and unreasonable . . . . The government's retention of all imaged electronic documents, including personal emails, without any review whatsoever to determine not only their relevance to this case, but also to determine whether any recognized legal privileges attached to them, is unreasonable and disturbing . . . .

Id. at 215 (emphasis in original). The court emphasized this failure to *commence* the analysis of the drives, rather than to *complete* it. *Id.* at 214. *Cf. United States v. Jarman*, 847 F.3d 259, 267 (5th Cir. 2017) (distinguishing *Metter* on ground that the government timely completed its review of seized evidence); *United States v. An*, 733 F. Supp. 3d 77, 106 (E.D.N.Y. 2024) ("unlike in *Metter*, which concerned an undue delay in commencing review, the Government here commenced its review the day the material became available") (emphasis in original); *see also United States v. Washington*, No. 23-CR-6109, 2024 WL 4750372, at *4 (W.D.N.Y. Nov. 12, 2024).

But beyond *Metter* and this handful of decisions distinguishing it, there is almost no developed law on this subject. The circuits have not articulated what factors govern the reasonableness inquiry when the government delays initiating—not merely completing—a review of seized digital evidence. Nor have they addressed how the government's candor with the supervising magistrate bears on that analysis. The absence of an "established upper limit," *Metter*, 860 F. Supp. 2d at 215, has left lower courts without a method to distinguish legitimate forensic delays from constitutionally intolerable government inaction.

The decision below illustrates the problem. The Ninth Circuit panel acknowledged the seven-month delay and conducted a Fourth Amendment reasonableness analysis, holding that the delay "did not violate the Fourth Amendment." App. A at 3. But the panel applied no approach specific to the digital-device context, and it did not engage with the distinction between initiating and completing a search that *Metter* and its progeny have recognized. Instead, the panel relied on *United States v. Johnson*, 875 F.3d 1265, 1276 (9th Cir. 2017), which held that a one-year delay between seizure and the issuance of a search warrant was not unreasonable. App. A at 3. But *Johnson* addressed how long the government can wait before seeking a warrant to search a seized item. 875 F.3d at 1275. Here, the government already had the warrant. It simply failed to act on it—failing even to transport the phones to a forensic laboratory for more than 200 days. 1-ER-24; 2-ER-276, 278. The panel did not grapple with that distinction, nor did it articulate any principle for evaluating whether the government's complete inaction during that period was constitutionally permissible.

B. The absence of a governing standard creates a risk of unchecked government delay.

The practical consequences of the absence of guidance from this Court are significant. Without an approach distinguishing between justified forensic delays and unjustified government inaction, the government has little incentive to initiate timely review of seized digital evidence. Under the approach taken by the appellate court, the government may seize a phone, take no steps to review it for months, allow a court-imposed deadline to lapse, obtain an extension by citing boilerplate

justifications, and face no consequences—so long as a reviewing court ultimately deems the total elapsed time "reasonable" in hindsight.

This case illustrates the danger. The March 19 warrant imposed a 120-day window for the government to complete its search of petitioner's phones. 2-ER-137. The government took no action during that entire period. It did not transport the phones to a laboratory. It did not begin any forensic analysis. 1-ER-24; 2-ER-276, 278. When the deadline passed, the government applied ex parte for a 120-day extension, attributing the delay to an "extensive backlog of devices to review" and the fact that "the forensic review of digital devices is time consuming." 2-ER-270. It did not disclose to the magistrate that no review had been initiated—or that the phones had not even been submitted for analysis. 2-ER-270–71. That fact only became clear when the defense received discovery concerning the dates on which the phones had been transported and analyzed by the forensics lab.

The panel credited the extension application at face value, finding that the government's request "provided sufficient reasons explaining the need for additional time, including an evidence backlog, one phone's sophisticated encryption software, and the diversion of resources to investigate a related case." App. A at 3. And it concluded that petitioner "offers no evidence that the government deliberately tarried or misled the court when it requested the extension." App. A at 4. But the record tells a different story. The government allowed a judicial deadline to expire without taking any action, then sought additional time without revealing that fact. Moreover, once the extension was granted, both phones were transported to the laboratory and the

forensic reviews completed within weeks. 2-ER-276, 278. If the backlog and technical constraints cited in the extension application were genuine, the rapid post-extension turnaround is difficult to explain.

This is precisely the kind of government conduct that *Metter* found constitutionally unacceptable: "blatant disregard" for the government's obligation to review seized data, compounded by indefinite retention of highly personal digital information "without any review whatsoever." 860 F. Supp. 2d at 215. The panel below effectively treated the government's months of total inaction as a legitimate forensic delay, which is what *Metter* rightly warns against. *Id.* at 214.

At minimum, this record called for an evidentiary hearing to explore the reasons for the government's inaction and the completeness of its disclosures to the magistrate.

C. The good-faith exception was misapplied.

The panel's alternative holding—that the good-faith exception to the exclusionary rule would apply even if a Fourth Amendment violation occurred, App. A at 3–4—compounded the error. The panel held that suppression is warranted only where police conduct is "deliberate, reckless, or grossly negligent," App. A at 4 (quoting *United States v. Jobe*, 933 F.3d 1074, 1079 (9th Cir. 2019)), and concluded that agents reasonably relied on the magistrate judge's extension order. App. A at 3–4. But the panel applied that standard without meaningfully examining the record, which showed that the government allowed a judicial deadline to expire without taking any steps to comply with it, 1-ER-24; 2-ER-276, 278, and then obtained an

extension through an application that omitted the most salient fact, 2-ER-270–71. As this Court has recognized, the exclusionary rule must apply where police misconduct is "sufficiently deliberate that exclusion can meaningfully deter it" and "such deterrence is worth the price paid by the justice system." *Herring v. United States*, 555 U.S. 135, 144 (2009). The government's course of conduct here—months of complete inaction followed by an incomplete disclosure to the court—is precisely the kind of conduct the exclusionary rule is designed to deter.

Moreover, while it is true that the agents who conducted the original search may not themselves have obtained the warrant extension, the forensics laboratory acted directly at the request of the prosecution to extract the contents of the phones. This scenario warrants different treatment from the usual analysis under *United States v. Leon*, 468 U.S. 897 (1984). Agents in the field executing a search warrant may be insulated from the prosecutor's knowledge that the warrant is deficient, but petitioner is aware of no case law suggesting that a forensics laboratory occupies the same position as an agent conducting a search in the field pursuant to a warrant specifying the place and objects to be searched. A forensics laboratory presumably never sees the search warrant and cannot, therefore, act in good-faith reliance on it. Rather, the laboratory simply receives a device with a request to extract its contents. The logic of the good-faith requirement simply does not apply in this situation. This, too, is a novel issue on which this Court should provide guidance to the courts below.

II. The Court Should Grant Certiorari to Address the Standard for Establishing Probable Cause to Search a Residence for Evidence of a Discrete, Completed Fraud.

While there is extensive case law addressing whether and when evidence is sufficiently stale to defeat a warrant, few authorities have addressed the question in the context of allegations of identity fraud that is not likely to be ongoing at the time a warrant is executed. The decision below illustrates the need for further guidance in this context.

The panel upheld the March 12 warrant based on evidence that petitioner paid an apartment application fee with his credit card while the rental application listed another person's personal identifying information, and on Agent Wong's testimony—based on his training and experience—that identity thieves keep evidence of their crimes in their residences. App. A at 2. In doing so, the panel applied a probable cause analysis developed for ongoing criminal activity such as drug sales or possession of child pornography.

This Court has required that facts supporting probable cause be "so closely related to the time of the issue of the warrant as to justify a finding of probable cause at that time." *Sgro v. United States*, 287 U.S. 206, 210 (1932). Courts have recognized that evidence of ongoing criminal enterprises may retain its force over time. *See United States v. Gann*, 732 F.2d 714, 722 (9th Cir. 1984). But a fraudulent lease application is a discrete, completed act. Once it is submitted, there is no reason to believe that evidence of the fraud will be stored at the residence, as might drugs or pornographic images. The affidavit here did not allege multiple victims, multiple

fraudulent applications, or any continuing scheme—only a single use of another person's identifying information to rent one apartment. 2-ER-154–58. Yet the panel credited Wong's affidavit that identity thieves "keep evidence of their crimes" at home without engaging with whether that assertion had any basis in the facts of this case. App. A at 2. Lower courts need guidance on whether—and under what circumstances—such generalized testimony can supply probable cause to believe that a completed offense will result in evidence maintained at the residence.

The affidavit was also insufficient on its own terms. It did not allege that petitioner himself had filled out or submitted the application. 2-ER-156. It gave no indication of whether C.W. had been contacted or had denied authorizing the use of his information. *Id.* It did not allege when the application had been submitted. *Id.* And it alleged no facts foreclosing obvious innocent explanations—such as that C.W. had authorized petitioner to use his information or had rented the apartment on petitioner's behalf. An affidavit that recites facts equally consistent with lawful conduct does not establish "a fair probability" of criminal activity; it establishes only suspicion. *Illinois v. Gates*, 462 U.S. 213, 238–39 (1983). Without guidance from this Court, lower courts will continue to uphold warrants based on ambiguous facts supplemented by boilerplate assertions from affiants about how criminals generally behave—effectively collapsing the probable cause requirement for discrete fraud offenses into a rubber stamp.

CONCLUSION

The petition for a writ of certiorari should be granted.

Respectfully submitted,

Date: April 8, 2026

/s/ Steven A. Brody

STEVEN A. BRODY
State Bar No. 271616
155 N Lake Ave, Ste 800
Pasadena, CA 91101
T: 213-290-5294
F: 213-403-5323
stevebrodylaw@gmail.com

Attorney for Petitioner