

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TENNESSEE
AT CHATTANOOGA

UNITED STATES OF AMERICA,)
)
 Plaintiff,) Case No. 1:26-CV-93
)
 v.) Judges
)
 6.03910214 BTC FROM COINBASE)
 ACCOUNT # xxxxxxxxxxxxxxxxxxxx5668e)
 IN THE NAME OF LINDA WINDER;)
)
 0.047749 USDC FROM COINBASE)
 ACCOUNT # xxxxxxxxxxxxxxxxxxxx5668e)
 IN THE NAME OF LINDA WINDER;)
)
 0.00587023 ETH FROM COINBASE)
 ACCOUNT # xxxxxxxxxxxxxxxxxxxx5668e)
 IN THE NAME OF LINDA WINDER,)
)
 Defendants.)

**AFFIDAVIT IN SUPPORT OF
VERIFIED COMPLAINT *IN REM***

I, Sean D. Reid, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been since 2018. I am currently assigned to the Nashville Division of the FBI. In this capacity, I am charged with investigating possible violations of federal criminal law. By virtue of my FBI employment, I perform and have performed a variety of investigative tasks, including functioning as a case agent on criminal cases. At the start of my employment, I received training on how to conduct criminal investigations at the FBI Academy in Quantico, Virginia. I have also received

training and gained experience in interviewing and interrogation techniques, the execution of federal search warrants, seizures, and the identification and collection of evidence. From my training and experience, I have also become familiar with the techniques and methods utilized by criminal enterprises to evade law enforcement while conducting criminal activity, to include ways to launder proceeds from illicit activity or forms of communication utilized to avoid law enforcement detection. In addition, I have worked with and consulted numerous agents and law enforcement personnel who have conducted complex criminal enterprise investigations within and outside the United States.

2. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, individuals, and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested purpose. It does not set forth all my knowledge or information known to law enforcement regarding this matter.

PURPOSE OF AFFIDAVIT

3. This affidavit is submitted in support of an application for a Verified Complaint *in Rem* for the following assets (“**the Subject Funds**”):

- a) 6.03910214 BTC from Coinbase account # xxxxxxxxxxxxxxxxxxxx5668e in the name of Linda Winder;
- b) 0.047749 USDC from Coinbase account # xxxxxxxxxxxxxxxxxxxx5668e in the name of Linda Winder; and
- c) 0.00587023 ETH from Coinbase account # xxxxxxxxxxxxxxxxxxxx5668e in the name of Linda Winder.

4. As set forth below, I submit there is probable cause to believe that the SUBJECT FUNDS constitute proceeds from violations of 18 U.S.C. §§ 1343, 1349, 1956, and 1957. The SUBJECT FUNDS are, therefore, subject to forfeiture to the United States.

FORFEITURE AUTHORITY

5. The SUBJECT FUNDS are subject to forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(C), on the grounds that the funds contained in the above-listed accounts constitute proceeds that are directly traceable to violations of 18 U.S.C. § 1343, 1349, 1956, and 1957. The SUBJECT FUNDS are further subject to forfeiture to the United States pursuant to 18 U.S.C. §§ 981(a)(1)(C) and 981(a)(1)(A), on the grounds that the funds contained in the above-listed wallets constitute proceeds that are directly traceable to violations of 18 U.S.C. §§ 1956 AND 1957. For reasons set forth below, probable cause exists for forfeiture of the SUBJECT FUNDS.

INVESTIGATION BACKGROUND

6 As further described below, this affidavit is made in support of an Verified Complaint *in Rem* for funds traceable to, and involved in, a fraud scheme involving the laundering of funds stolen from a nonprofit organization victimized in a business email compromise (BEC) that resulted in a loss of approximately \$2.6 million. The laundering of these stolen funds was conducted by an individual (or individuals) participating in a role commonly referred to as a “money mule.” A money mule is someone who transfers illegally acquired money on behalf of or at the direction of another. Money mules are often recruited via an online romance or online job scheme. Criminals use money mules to move money electronically through bank accounts. They are asked by the criminal actors to use an established bank account or open a new bank account to

receive money from someone they have never met in person. They may also be asked to move physical currency, or to assist the movement of money through a variety of other methods such as wiring the money into a third-party bank account, “cashing out” the money received via currency or cashier’s checks, converting the money to virtual currency (such as Bitcoin), converting the money to prepaid cards (such as debit cards or gift cards), sending the money through a money service business (such as Western Union or MoneyGram) or a money transmitting app (such as Venmo or Zelle), or a combination of these. The money mule may be told to keep a portion of the money being transferred. Money mules add layers to the money trail from a victim to a criminal actor.

7. Money mules can be witting and complicit in the transfer of the illegally acquired money. The money mule may ignore obvious red flags or act willfully blind to the money movement activity. The money mule may have been warned about the activity by a bank employee or law enforcement. The money mule may serially open bank accounts because prior bank accounts had been closed by banks due to the suspicious activity in the accounts. The money mule’s motivation may be financial gain or misplaced loyalty to a criminal actor.

8. Criminal actors obtain money through various illegal acts, and they need someone to move this money at their direction. Common criminal activities include romance scams, work-from-home scams, mystery shopper scams, lottery scams, Business Email Compromise, reshipping scams, Internal Revenue Service (IRS) or law enforcement impersonation scams, credit card fraud, and drug trafficking. Money mules help criminals launder their criminally derived proceeds by adding layers of recipients to the money trail, and these layers complicate and negatively impact the ability of law enforcement to accurately trace the money from a specific victim to a criminal actor.

9. In this instance, the money mule acting on behalf of a person or persons unknown received multiple deposits of tens and hundreds of thousands of dollars over a period of several months, totaling approximately \$1.4 million, which she then laundered by transferring to the Coinbase Account, one of many financial accounts used in laundering of these stolen funds and converting to cryptocurrency.

10. Based on my training and experience and the facts as set forth in this affidavit, I respectfully submit that there is probable cause to believe that the owner of **the Coinbase Account**, operating under the direction and guidance of unknown subjects, violated 18 U.S.C. §§ 1343 and 1349 (wire fraud and conspiracy to commit wire fraud) and laundered the proceeds of that activity in violation of 18 U.S.C. §§ 1956(a)(1)(B)(i), 1957, and 1956(h) (money laundering, violation of the spending statute, and conspiracy to commit money laundering). 18 U.S.C. § 1956(a)(1)(B)(i) makes it a crime to conduct or attempt to conduct a financial transaction, knowing that the property involved in the transaction represents the proceeds of some form of unlawful activity, and which in fact involves the proceeds of specified unlawful activity, knowing that the transaction is designed in whole or in part to conceal the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity. 18 U.S.C. § 1957 provides in relevant part that “[w]hoever... knowingly engages or attempts to engage in a monetary transaction in criminally derived property of a value greater than \$10,000 and is derived from specified unlawful activity” shall be guilty of a federal offense. Because the offense consists of spending the proceeds of specified unlawful activity, § 1957 is sometimes referred to as the Spending Statute. Violations of § 1957 are considered money laundering offenses.

11. There is also probable cause to believe that **the Coinbase Account** received the proceeds of the wire fraud scheme described below and that **the Subject Funds** are subject to

forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C). Moreover, there is probable cause to believe that **the Subject Funds** are subject to forfeiture as property involved in money laundering offenses and proceeds, pursuant to 18 U.S.C. §§ 981(a)(1)(A) and 981(a)(1)(C).

PROBABLE CAUSE

12. In October 2023, a family member of Athens, Tennessee resident Linda Winder reported finding an envelope in Winder's home containing a series of deposit slips from cryptocurrency kiosks totaling approximately \$162,730 worth of Bitcoin. These receipts appeared to have been attempted to be sent by Winder to an individual unknown to the reporting party. The family member disclosed that since Winder's husband had died in 2017, many individuals had contacted Winder online, identifying themselves as single men, and in 2019 Winder ultimately had begun an online relationship with one such person going by the name of Joe Milano. The family member reported that Winder had wired money to Milano as part of a romance scam and was concerned she was also laundering money.

13. The FBI conducted multiple interviews of Winder and her family during which, Winder and family members described a scheme in which Milano gradually coaxed Winder to send him money, initially from her own funds in increasing amounts, before eventually directing Winder to open at least one account at a cryptocurrency exchange. Winder and her family advised that Winder had taken out several personal loans totaling \$150,000 and withdrawn approximately \$33,000 of her own money for funds which she sent to Milano. Separately, Winder acknowledged that she had transacted hundreds of thousands of dollars in person through her Wells Fargo Bank account on Milano's behalf. In fact, the FBI learned that Winder had used accounts at several financial institutions to transfer money received fraudulently from other parties, to include

unknown third parties. Winder then forwarded the money at the behest or direction of Milano to her cryptocurrency account or through cryptocurrency kiosks to a cryptocurrency exchange, or to other financial institutions or individuals. The FBI believes that over the course of Winder's relationship with Milano, between 2021 and 2023, Winder participated in the laundering of no less than \$2.3 million.

14. Winder used **the Coinbase Account**, which Coinbase froze due to her suspected fraudulent activity. The FBI requested Coinbase maintain its freeze of the funds in **the Coinbase Account**. On January 18, 2024, Coinbase complied with the FBI's request and advised the frozen funds in the Subject Address were valued at \$249,068.00. On April 15, 2025, Coinbase advised the FBI the value of the funds in the frozen account had more than doubled, to stand at \$510,155.96.

15. In August 2023, the FBI was notified of a business email compromise of a Minnesota-based nonprofit organization ("Victim Company") dedicated to supporting individuals with disabilities across the state, to include transportation and home-based services. The Victim Company was a significant client of Lyft's rideshare services and was paying Lyft approximately \$500,000 per month. Beginning around January 2023 and continuing for several months, an unknown subject ("UNSUB") gained access to at least one Victim Company email account. The UNSUB then created the fraudulent email account `accountsreceivable@lyftinc.com` ("lyftinc.com") which was very similar to the legitimate Lyft email account `accountsreceivable@lyft.com` ("lyft.com"). The UNSUB created rules within the Victim Company's email accounts to delete legitimate emails from `lyft.com`, so the Victim Company would only see the fraudulent invoices from the UNSUB via email account `lyftinc.com` along with the UNSUB's ACH payment instructions. At the same time, the UNSUB was sending emails to

Lyft impersonating the Victim Company and telling Lyft the delays in remittance were due to waiting to receive state funds, allowing the UNSUB to continue defrauding the Victim Company. Lyft also allowed accounts like the Victim Company that were state programs with federally funded welfare dollars to go into arrears for nine months before addressing non-payment. In August 2023, an employee of the Victim Company noticed an email from lyft.com come into his inbox and immediately disappear. The employee found the email in his deleted emails and then discovered the rule within the email platform created by the UNSUB which revealed the entire fraud. In total, the UNSUB defrauded the Victim Company of approximately \$2.6 million.

16. The FBI identified deposits occurring between March and July 2023 totaling approximately \$1.4 million in stolen funds from the Victim Company deposited directly to a Wells Fargo bank account owned and controlled by Winder. Of these funds, approximately \$1.165 million were deposited between April and June 2023 into **the Coinbase Account**.

17. During her initial FBI interview on October 30, 2023, Winder told agents that none of the money in the Coinbase account was hers and that it all belonged to Milano or other individuals.

18. Additionally, in July 2023, following the same April to June 2023 time period in which the Victim Company's funds were being transferred from Winder's Wells Fargo bank account to **the Coinbase Account**, \$178,046 of those stolen funds were deposited separately to two Oak Ridge National Laboratory (ORNL) Federal Credit Union (FCU) accounts in July 2023, also owned by Winder:¹ \$163,046 to one ("ORNL FCU Account 1") and \$15,000 to another

¹ The listed text in Line 16 clarifies the nature of transfers from Winder's Wells Fargo account to the two listed ORNL FCU accounts, corrected from the previous affidavit (1:25-MJ-144; Signed June 06, 2025). In the previous affidavit, the affiant attested to \$183,586 in stolen funds being deposited to Winder's ORNL FCU accounts in or around April to June 2023. While these funds were highlighted in the FBI's financial accounting as occurring during the same relative time frame as the BEC transfer of funds to the Wells Fargo account, the ORNL deposits specified herein totaled \$178,046 and occurred in July 2023.

(“ORNL FCU Account 2”). Between July and August 2023, approximately \$166,550 in cash withdrawals were made from ORNL FCU Account 1. In July 2023, the \$15,000 in ORNL FCU Account 2 was withdrawn two days after it was transferred into the account. These cash withdrawals from the two ORNL FCU accounts totaled approximately \$181,550.

19. In or around the same July to August time period, Winder made cash deposits to cryptocurrency kiosks totaling approximately \$162,730, as identified through the cryptocurrency kiosk deposit receipts discovered by Winder’s family member. Through tracing efforts, the FBI has learned the money deposited into the cryptocurrency kiosks was converted to Bitcoin and transferred to two offshore, foreign-held cryptocurrency accounts and unrecoverable. The outstanding cash remaining from the multiple ORNL FCU withdrawals here too consists of the same \$1.4 million stolen from the Victim Company which was initially deposited to Winder’s Wells Fargo account. The FBI has identified a remaining balance of approximately \$18,820 of this stolen money that was withdrawn by Winder in cash and is as of yet still unaccounted for.²

20. Winder further sought to conceal the nature, source, and ownership, of the proceeds of this specified unlawful activity. In at least seven wire transactions to Coinbase, occurring between April 7 and June 30, 2023, Winder masked the purpose of these transactions using untrue statements as to their purpose, such as, the following: “medical expenses” (\$136,500 on April 7,

² FBI tracing revealed Winder also transmitted approximately \$55,000 to third parties in July 2023. The outstanding, approximately \$18,820 in unaccounted cash withdrawals was derived against the Bitcoin ATM receipts (totaling \$162,730) created at or around the same approximate time frame as Winder’s cash withdrawals from the two ORNL FCU accounts (\$181,550). To summarize, Winder received \$1,403,222.36 to her Wells Fargo account from the Victim Company, of which she sent \$1,165,468.87 to Coinbase and \$178,046 to two ORNL FCU accounts from which she made \$181,550 in withdrawals that the FBI contends were used in the purchase of at least \$162,730 in Bitcoin. These transactions, combined with the \$55,000 sent to third parties, total \$1,398,514.87 in laundered money. At the time of this application, an FBI financial investigator has been engaged to determine Winder’s liability for any unaccounted funds that can be traced to the initial \$1.4 million in stolen money she received in the BEC of the Victim Company.

2023); “investment purposes” three times (\$152,750 on April 20, 2023, \$148,320 on May 08, 2023, and \$163,720 on May 22, 2023; as well as \$193,370 as an “investment” on June 30, 2023); “personal expenses” (\$193,480.87 on June 05, 2023); “closing on a home” (\$127,328 on June 22, 2023). In Winder’s July 14, 2023, transfer (\$150,046) from her Wells Fargo account to one of the two ORNL FCU accounts referenced earlier, “switching banks to one closer to home” was the explanation provided.³

21. On June 06, 2025, the seizure warrant 1:25-MJ-144 was served to Coinbase for funds equal to the amount held in Winder’s frozen Coinbase account. On June 09, 2025, Coinbase confirmed receipt of the warrant and provided the following account balances, then valued at \$655,205.79:

Bitcoin (BTC) Wallet; 6.03910214
USDC Wallet; 0.047749
Ethereum (ETH) Wallet; 0.00587023

On June 17, 2025, the FBI submitted a request for a direct transfer of funds from the captioned account to the U.S. Marshals Service (USMS). The USMS advised it would deny the transfer of USDC as its value was below a threshold amount for seizure (approximately \$0.04).

22. On June 24, the USMS provided a wallet address to receive both the Bitcoin and Ethereum cryptocurrency in the Coinbase account. On July 16, 2025, Coinbase successfully sent approximately \$20 worth of BTC (.00016805) in a test transfer to the USMS. On July 18, 2025, Coinbase successfully transferred the remaining, outstanding balance of Bitcoin to the USMS, for a total balance of 6.03908019 BTC and approximate value of \$712,630 at time of receipt. No further transfers had been made from Winder’s Coinbase account to the USMS, pending an

³ The listed text in Line 18 clarifies the July 14 transfer of funds as occurring between Winder’s Wells Fargo and ORNL FCU accounts, which was not specified in the previous affidavit (1:25-MJ-144; Signed June 06, 2025).

updated seizure warrant for the remaining Ethereum held in the frozen account. On August 28, 2025, the USMS advised the current dollar value of the remaining Ethereum in Winder's account stood at approximately \$26.

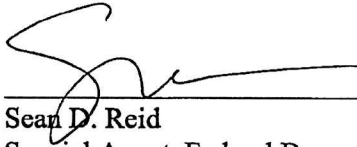
23. Said account is subject to seizure to United States pursuant to 18 U.S.C. § 981(b). Said account is also subject to civil forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C), on the grounds that the funds contained in the above-listed account constitutes proceeds that are directly traceable to offenses in violation of 18 U.S.C. § 1343 (wire fraud) and 18 U.S.C. § 1349 (conspiracy to commit wire fraud). The account is further subject to civil forfeiture under 18 U.S.C. §§ 981(a)(1)(A) and 981(a)(1)(C) as it is involved in and contains proceeds that is directly traceable to and facilitated the offense in violation of 18 U.S.C. §§ 1956(a)(1)(B)(i), 1957, and 1956(h) (money laundering).

CONCLUSION

24. The subject property constitutes proceeds that are directly traceable to violations of 18 U.S.C. §§ 1343 and 1349 and is subject to civil forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C) and constitutes property involved in or traceable to a transaction or attempted transactions in violation of 18 U.S.C. §§ 1956 and 1957 and is subject to civil forfeiture pursuant to 18 U.S.C. §§ 981(a)(1)(A) and 981(a)(1)(C).

All of the above information is true and correct to the best of my knowledge.

FURTHER THIS AFFLIANT SAYETH NOT



Sean D. Reid
Special Agent, Federal Bureau of Investigation

STATE OF TENNESSEE

COUNTY OF Knox

On this 31st day of March, 2026, before me, personally appeared Sean D. Reid in his capacity as a Special Agent with the Federal Bureau of Investigation, to me known to be the person described in and who executed the foregoing instrument, and acknowledged that he executed the same as his free act and deed.

IN WITNESS WHEREOF I have hereunto set my hand and Notarial Seal.

Subscribed to and sworn before me on this this 31st day of March, 2026.



NOTARY PUBLIC

My Commission Expires: 01/30/2030