IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NORTH CAROLINA
CHARLOTTE DIVISION

CASE NO. 3:26-cv-00834

| | |
|---|---|
| UNITED STATES OF AMERICA<br><br>v.<br><br>ALL CIRCLE USD COIN (USDC) STORED IN THE FOLLOWING ADDRESS ON THE ETHEREUM BLOCKCHAIN<br>0xE6d328eB45Bd03B2cbb801a0c4a93c993F735b76. | **COMPLAINT FOR FORFEITURE *IN REM*** |

NOW COMES the United States of America, Plaintiff herein, by and through Russ Ferguson, United States Attorney for the Western District of North Carolina, in a civil cause of forfeiture, and respectfully states the following:

## INTRODUCTION

1. This action seeks the forfeiture of all Circle USD Coin ("TARGET USDC"), stored in the following un-hosted blockchain address held on the Ethereum Blockchain: 0xE6d328eB45Bd03B2cbb801a0c4a93c993F735b76 ("TARGET ADDRESS"). As of September 23, 2026, the balance of the TARGET ADDRESS was approximately 119,306.268701 USDC.

2. I respectfully submit that the TARGET USDC is proceeds of a wire fraud conspiracy and scheme, whereby individuals obtained purported investments and other payments from a victim, and then directed the assets to the TARGET ADDRESS. In summary, one or more individuals contacted victim "A.M." and convinced A.M. to wire cryptocurrency into a Bifrost Wallet in order to obtain investment returns. Thereafter, without A.M.'s consent, the individual/s removed A.M.'s cryptocurrency from the wallet to the TARGET ADDRESS. The individual/s advised A.M. that the cryptocurrency was removed due to suspected involvement in crime, and

duped A.M. into paying even more cryptocurrency into the wallet in order to "verify" the funds so that the cryptocurrency could be released to A.M. The individual/s who had contacted A.M. did not release the cryptocurrency. Subsequently, law enforcement traced the fraud on A.M. to the TARGET ADDRESS, and obtained and executed a warrant for the TARGET USDC. Law enforcement has now identified numerous victim complaints of fraud, in addition to Victim A.M.'s complaint, that bear indicia of the fraud against Victim A.M. and are related to one or more of the same accounts, addresses, and/or websites discussed herein.

3. This is a civil action *in rem* pursuant to 18 U.S.C. § 981(a)(1)(C). Procedures for this action are mandated by Rule G of the Supplemental Rules for Admiralty or Maritime Claims and Asset Forfeiture Actions and, to the extent applicable, 18 U.S.C. §§ 981, 983, and 984, and the Federal Rules of Civil Procedure.

4. The cryptocurrency constitutes or is derived from proceeds of wire fraud conspiracy and wire fraud in violation of 18 U.S.C. §§ 1343 and 1349.

5. This Court has jurisdiction over this action commenced by the United States under 28 U.S.C. § 1345 and over this action for forfeiture under 28 U.S.C. § 1355(a). The Court has in rem jurisdiction over the defendant property under 28 U.S.C. § 1355(b).

6. This Court has venue pursuant to 28 U.S.C. §§ 1355 and 1395. Venue is proper because the acts or omissions giving rise to the forfeiture occurred in this district, the claim accrued in this district, and federal law enforcement controls the cryptocurrency in this district.

7. Specifically, on or about June 13, 2025, the Federal Bureau of Investigation ("FBI"), served on Circle Internet Financial, LLC ("Circle") a federal Warrant to Seize Property Subject to Forfeiture for the TARGET USDC contained in the TARGET ADDRESS. Then, in September 2026, following negotiations between Circle and the United States, Circle entered into

a settlement to block the TARGET ADDRESS and issue replacement USDC to the United States if the Court orders final forfeiture in this action.

8. Pursuant to Supplemental Rule G(2)(f), facts in support of a reasonable belief that the Government will be able to meet its burden of proof at trial are set forth more fully as follows and have been verified by the attached Verification of FBI Special Agent Courtney Richardson.

## BACKGROUND ON CRYPTOCURRENCY

9. The following relevant terms and definitions pertain to the cryptocurrency and conduct described in this Complaint:

a. **Cryptocurrency**, a type of virtual currency, is a decentralized, peer-to-peer, network-based medium of value or exchange that may be used as a substitute for fiat currency to buy goods or services or exchanged for fiat currency[1] or other cryptocurrencies. Examples of cryptocurrency are Bitcoin, Litecoin, Ether and USD Coin (USDC). Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or in cloud-based servers. Although not usually stored in any physical form, public and private keys (described below) used to transfer cryptocurrency from one person or place to another can be printed or written on a piece of paper or other tangible object. Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange, or through other intermediaries. Generally, cryptocurrency is not issued by any government, bank, or company; it is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Most cryptocurrencies have a "blockchain," which is

[1] Fiat currency is currency issued and regulated by a government such as the U.S. Dollar, Euro, or Japanese Yen.

a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction.[2]

b. A **blockchain** is a digital ledger run by a decentralized network of computers referred to as "nodes." Each node runs software that maintains an immutable and historical record of every transaction utilizing that blockchain's technology. Many digital assets, including virtual currencies, publicly record all of their transactions on a blockchain, including all of the known balances for each virtual currency address on the blockchain. Blockchains consist of blocks of cryptographically signed transactions, and blocks are added to the previous block after validation and after undergoing a consensus decision to expose and resist tampering or manipulation of the data. There are many different blockchains used by many different virtual currencies. For example, Bitcoin in its native state exists on the Bitcoin blockchain, while Ether (or "ETH") exists in its native state on the Ethereum network.

c. **Stablecoins** are a type of virtual currency whose value is pegged to a commodity's price, such as the gold price, or to a fiat currency, such as the U.S. dollar, or to a different virtual currency. For example, USDC is a stablecoin pegged to the U.S. dollar. Specifically, USDC is fully backed by an equivalent amount of U.S. dollar-denominated assets held by Circle Internet Financial, LLC ("Circle") with U.S. regulated financial institutions in segregated accounts apart from Circle's corporate funds, and for every USDC issued by Circle and remaining in circulation, Circle will hold on behalf of USDC users either one U.S. dollar ("USD") or an equivalent amount of USD-denominated assets (the "USDC

[2] Some cryptocurrencies operate on blockchains that are not public and operate in such a way to obfuscate transactions, making it difficult to trace or attribute transactions.

Reserves"). Stablecoins achieve their price stability via collateralization (backing) or through algorithmic mechanisms of buying and selling the reference asset or its derivatives

d. **Circle Internet Financial, LLC ("Circle")** is a company that manages the smart contracts and the treasury (*i.e.*, the funds held in reserve) for USDC tokens. Circle, as the issuer of USDC, has the technical ability to block individual addresses on the Ethereum blockchain from sending or receiving USDC, a process known as "blocklisting." The USDC from the blocklisted TARGET ADDRESS is referenced as the "Original USDC." The United States is not able to access the Original USDC because the blocklisted TARGET ADDRESS remains under the control of unknown parties. Circle advises that it not have the technical ability to transfer the Original USDC from the blocklisted TARGET ADDRESS to the United States, but has agreed to voluntarily issue new USDC in an amount equivalent to the amount of the Original USDC (the "Replacement USDC") and transfer the Replacement USDC to the United States.

e. Individuals can acquire USDC through exchanges (i.e. online companies which allow individuals to purchase or sell cryptocurrencies in exchange for fiat currencies or other cryptocurrencies), cryptocurrency ATMs, or directly from other people. Coinbase, Inc. ("Coinbase") is an example of an exchange where individuals can purchase cryptocurrency. Individuals can send and receive cryptocurrencies online using many types of electronic devices, including laptop computers and smart phones. Even though the public addresses of those engaging in cryptocurrency transactions are recorded on a blockchain, the identities of the individuals or entities behind the public addresses are not recorded on these public ledgers. If, however, an individual or entity is linked to a public address, it may be possible to determine what transactions were conducted by that

individual or entity. USDC transactions are therefore sometimes described as "pseudonymous," meaning that they are partially anonymous. And while it is not completely anonymous, USDC allows users to transfer funds more anonymously than would be possible through traditional banking and financial systems.

f. Cryptocurrency is stored in a virtual account called a wallet. **Wallets** are software programs that interface with blockchains and generate and/or store public and private keys used to send and receive cryptocurrency. A **public key** or **address** is akin to a bank account number, and a **private key** is akin to a PIN number or password that allows a user the ability to access and transfer value associated with the public address or key. To conduct transactions on a blockchain, an individual must use the public address (or "public key") and the private address (or "private key"). A public address is represented as a case-sensitive string of letters and numbers, 26–42 characters long. Each public address is controlled and/or accessed through the use of a unique corresponding private key—the cryptographic equivalent of a password or PIN—needed to access the address. Only the holder of an address' private key can authorize any transfers of cryptocurrency from that address to another cryptocurrency address. Although cryptocurrencies such as Bitcoin have legitimate uses, cryptocurrency is also used by individuals and organizations for criminal purposes such as money laundering and is an oft-used means of payment for illegal goods and services. By maintaining multiple wallets, those who use cryptocurrency for illicit purposes can attempt to thwart law enforcement's efforts to track transactions.

g. Law enforcement can trace transactions on blockchains to determine which virtual currency addresses are sending and receiving particular virtual currency. This analysis can be invaluable to criminal investigations for many reasons, including that it may enable law

enforcement to uncover transactions involving illicit funds and to identify the person(s) behind those transactions. To conduct blockchain analysis, law enforcement officers use reputable, free open-source blockchain explorers, as well as commercial tools and services. These commercial tools are offered by different blockchain-analysis companies. Through numerous unrelated investigations, law enforcement has found the information associated with these tools to be reliable.

## FACTS

10. On June 10, 2025, an individual identified herein as "A.M.," a 69-year old resident of Charlotte, North Carolina, contacted the FBI to report that he was a victim of a cryptocurrency investment scheme in which he lost approximately $150,000. Subsequently, law enforcement interviewed A.M. on multiple occasions and collected documentary and electronic evidence from A.M. These interviews and documents reflected the following timeline of events.

11. On approximately March 30, 2025, A.M. met an individual purporting to be "Thalia Williams" ("Williams") via social media website, X. Williams and A.M. primarily communicated through various messaging applications to include X chat and WhatsApp.

12. Williams told A.M. about an investment opportunity where he could earn daily interest on funds in a cryptocurrency wallet. Williams directed A.M. to download the Bifrost Wallet App and provided A.M. directions on how to link his Bifrost Wallet to qsjt66.com, which generated the daily interest payments based on the amount of funds in A.M.'s Bifrost Wallet. Qsjt66.com advertised unrealistic daily interest rates; for example, a wallet balance between 500,001 and 1,000,001 would earn a daily interest rate of 3.3%.[3]

[3] A daily interest rate of 3.3% would equate to an annual percentage rate (APR) of approximately 1,204%. Legitimate investment portals do not offer such extraordinarily high rates of return.

13. Between approximately April 7, 2025 and May 27, 2025, A.M. **deposited a total of approximately 50,000 USDC into his Bifrost Wallet.** A.M. believed he would earn legitimate interest on the balance of the funds that A.M. deposited in his Bifrost Wallet, based on the rates advertised on qsjt66.com. In fact, between approximately April 7, 2025 and May 27, 2025, A.M. received a total of approximately 5,000 USDC deposited into his Bifrost Wallet; A.M. believed these deposits to be daily interest payments on the balance of his Bifrost Wallet.

14. One of the transfers made by A.M. into his Bifrost Wallet was a transfer on approximately May 27, 2025 for approximately 5,000 USDC.

15. On May 27, 2025, A.M. received the following message on qsjt66.com: "[h]ello, dear user, the system has detected that a fund suspected of money laundering (5007.442069 USDC) has arrived in your account. In order to protect the safety of your funds, we have locked your funds in the mining pool!" On or around the same day, all of the USDC in A.M.'s Bifrost Wallet, amounting to approximately 55,000 USDC, were transferred out of his Bifrost Wallet. A.M. did not initiate the transfer out of his Bifrost Wallet.

16. On May 29, 2025, A.M. received the following message on qsjt66.com: "[h]ello dear user! Please seek support from your dedicated support staff Tim, he will help you solve all these problems, his email is timereumtim@gmail.com." On or around the same day, A.M. emailed "Tim" at email address, timereumtim@gmail.com, and requested assistance on how to get A.M.'s funds returned. On or around the same day, A.M. received an email from address timereumtim@gmail.com. The sender purported to be "Tim" and identified himself as a customer service representative for Ethereum Network Investment. Tim told A.M. that the 5,000 USDC transfer was from unknown funds and suspected of money laundering, which caused A.M.'s account to be frozen. Tim stated that A.M. would be required to make verification

payments into his Bifrost Wallet in order for his missing funds to be released back into his Bifrost Wallet. On May 30, 2025, A.M. made two verification payments to his Bifrost Wallet. The same day, the funds were transferred out of A.M.'s Bifrost Wallet. A.M. did not initiate the transfer out of his Bifrost Wallet.

17. On June 2, 2025, A.M. again received an email from Tim at email address timereumtim@gmail.com. The email advised, in essence, that the verification payments were successful but that A.M.'s funds could not be released because the 5,000 USDC transfer was from a money laundering fund that had been locked by the FBI. Tim told A.M. that A.M. would have to make an additional verification payment before his funds could be released. On June 2, 2025, A.M. made a verification payment to his Bifrost Wallet. That same day, the funds were transferred out of A.M.'s Bifrost Wallet. A.M. did not initiate the transfer out of his Bifrost Wallet.

18. On June 2, 2025, A.M. received yet another email from Tim at email address timereumtim@gmail.com. Tim advised that the verification payment had been completed, but the payment was not for the correct amount, so A.M.'s funds could not be released. On June 5, 2025, A.M. made another verification payment to his Bifrost Wallet. That same day, the funds were transferred out of A.M.'s Bifrost Wallet. A.M. did not initiate the transfer out of his Bifrost Wallet.

19. In total, between approximately May 30, 2025 and June 5, 2025, A.M. **transferred approximately 100,000 USDC into his Bifrost Wallet for verification payments**.

20. On June 5, 2025, A.M. received an email from Tim at email address timereumtim@gmail.com that stated that the verification payment was successful. The same day, A.M. received another email from Tim at email address timereumtim@gmail.com that

advised, in essence that A.M. must pay a 20% tax for his mining pool funds before his funds could be released. On June 10, 2025, A.M. received yet another email from Tim at email address timereumtim@gmail.com that stated that if A.M. did not pay the taxes before Friday, his earnings would be suspended and his funds would be transferred to the IRS.

21. On May 30, 2025, the FBI received a complaint regarding a similar cryptocurrency investment fraud scheme. According to that complainant, an individual contacted the complainant on X and directed the complainant to download Bifrost Wallet and register qsjt66.com in the Bifrost Wallet. The complainant was notified his Bifrost Wallet was in a zombie state and that he would need to deposit additional funds to remove his account from a zombie state. The complainant was advised that, if the complainant did not deposit additional funds, then his funds from his Bifrost Wallet would be gone.

22. On June 5, 2025, the FBI received a complaint regarding another similar cryptocurrency investment fraud scheme. According to the complainant, an individual contacted the complainant on X and directed the complainant to invest using a Bifrost Wallet and qsjt66.com. The complainant reported that his Bifrost Wallet was hacked so his account was frozen, and verification payments would be required before his account could be unfrozen.

23. The initial communications to A.M. soliciting investments, as well as the follow-up communications from "Tim" soliciting payments to unfreeze assets and pay taxes, were indicative of a common scheme whereby fraudsters dupe victims into involvement in a scheme whereby an individual fraudulently convinces a victim to pay "insurance," "taxes," or purported law enforcement fees, all under the guise of obtaining the return of funds or a prize. During the execution of such a scheme, the fraudster will continue such conduct until the victim discovers the true nature of the scheme and ceases paying, at which point the fraudster has often already

started moving or laundering the fraud proceeds.

24. As a result of the suspicious communications to A.M. and the other complaints related to this matter, law enforcement conducted blockchain analysis tracing the victim's funds to the TARGET ADDRESS.

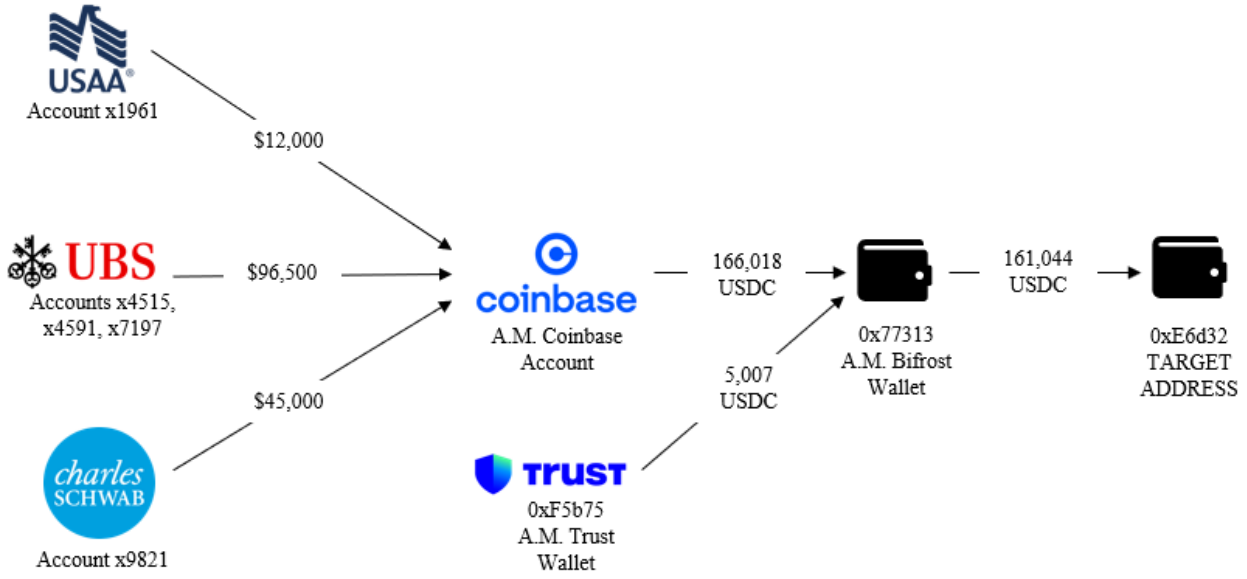
## TRACING OF VICTIM'S FUNDS

25. Based on publicly available blockchain information, the use of reliable commercial tools and services, and information provided by A.M., the specific flow of assets in this case was as follows.

26. As described in greater detail herein, A.M. created a Coinbase account, which he funded predominantly using his personal financial accounts at USAA, UBS, and Charles Schwab. A.M. subsequently sent funds from Coinbase and Trust Wallet to his Bifrost Wallet at virtual currency Address 0x77313 ("Address 0x77313")—the Bifrost Wallet that one or more individuals directed A.M. to create. From Address 0x77313, the funds moved to the TARGET ADDRESS.

27. The flow of funds from A.M. to the TARGET ADDRESS is illustrated below. Arrows used in illustrating the flow of funds between addresses may be representative of multiple

transactions. USDC amounts in this Affidavit are rounded to the nearest whole value. The virtual currency addresses here and elsewhere in this Affidavit are truncated for ease of reference.




28. The flow of funds graphically illustrated above is also described as follows:

a. Victim A.M. used his personal financial accounts at USAA (account ending x1961), Union Bank of Switzerland (UBS) (accounts ending x4515, x4591, and x7197), and Charles Schwab (account ending x9821) to fund a Coinbase account, which he owned and controlled. Between April 4, 2025 and June 5, 2025, A.M. conducted transfers totaling at least $153,500 from these personal financial accounts to his Coinbase account. Prior to April 4, 2025, A.M. had not conducted any transactions in his Coinbase account.

b. The deposits into A.M.'s Coinbase account funded the purchase of virtual currency, primarily USDC. The USDC was predominantly sent to Address

0x77313. In total, at least 166,018 USDC was deposited from A.M.'s Coinbase account into Address 0x77313.

c. A.M. also had a wallet with virtual currency Address 0xF5b75, utilizing Trust Wallet, a non-custodial wallet. A.M. used this wallet to send 5,007 USDC to Address 0x77313.

d. A review of the transaction activity in Address 0x77313 shows that, between April 7, 2025 and June 5, 2025, the Address received total deposits of 176,924 USDC. As described in the preceding paragraphs, the majority of these funds came from A.M.'s Coinbase account (166,018 USDC) and A.M.'s Trust wallet 0xF5b75 (5,007 USDC). The remaining deposits included many smaller value transactions, occurring on a near-daily basis, from various virtual currency addresses; A.M. believed these deposits to be interest payments received based on the balance of funds in Address 0x77313. Between May 27, 2025 and June 5, 2025, a total of four withdrawals were made from Address 0x77313, totaling 161,044 USDC. These withdrawals were deposited to the TARGET ADDRESS.

29. More broadly, between March 20, 2025 and June 12, 2025, the TARGET ADDRESS received 60 deposits totaling 369,306 USDC. **Of these deposits, 161,044 USDC was from A.M.'s Bifrost Wallet Address 0x77313 as described above.** Since then and as of June 12, 2025, only three withdrawals have been made from the TARGET ADDRESS, totaling 250,000 USDC.

30. As of the date of service of the federal Warrant to Seize Property Subject to Forfeiture, on or about June 13, 2025, the balance of the TARGET ADDRESS was 119,306

USDC. Based on the application of the "lowest intermediate balance rule" ("LIBR") accounting principle[4], the fraud on Victim A.M. funded approximately 117,648, equivalent to approximately 99% of the balance, of the USDC remaining in the TARGET ADDRESS as of June 13, 2025.

31. Subsequent to June 13, 2025, the FBI received additional complaints regarding similar cryptocurrency investment fraud schemes. Some of these complaints are indicative of the same conduct whereby one or more conspirators defrauded Victim A.M.

32. For example, one such complaint was received on June 22, 2025. According to the complainant, an individual contacted the claimant on X and directed the complainant to invest using a Bifrost Wallet and qsjt66.com. The complainant reported that their assets were frozen because they were accused of a malicious cash grab, and they would need to conduct additional deposits to verify the account. The complainant was advised that if they did not verify the account within 72 hours, their cryptocurrency would be donated to a cryptocurrency charity. The complainant stated that they sent cryptocurrency to 0xE6d328eB45Bd03B2cbb801a0c4a93c993F735b76, the TARGET ADDRESS. The complainant stated that they sent the cryptocurrency on June 9, 2025 (prior to the date of service of the federal Warrant to Seize Property Subject to Forfeiture, on or about June 13, 2025, at which time Circle blocklisted the TARGET ADDRESS). This complaint reinforces the FBI's initial analysis that one or more fraudsters directed assets from multiple victims, in addition to Victim A.M., into the TARGET ADDRESS and that at least approximately 99% of the balance of the TARGET ADDRESS is traceable to victim funds.

[4] According to this method, the amount in an account is traceable up to the amount of deposits of illegal funds into the account, regardless of withdrawals, as long as the balance does not drop below the total deposits of illegal funds. For instance, if an account containing $100 was comprised of $50 in clean funds and $50 in dirty funds and $75 was withdrawn, the government could assume the dirty funds exited last. The result would be that $25 in dirty funds remained in the account.

33. On June 18, 2025, Circle notified the FBI that Circle had received a third party inquiry related to the TARGET ADDRESS. Although Circle advised the inquirer on how to contact the FBI directly, the FBI did not receive any direct communications from third party inquirers about the TARGET ADDRESS. This absence of any contact between the holder of the TARGET ADDRESS and the FBI is indicative of an address holder engaged in fraud and reticent to make contact with law enforcement.

## CONCLUSION

34. By virtue of the foregoing and pursuant to 18 U.S.C. § 981(b), all right, title, and interest in the TARGET USDC vested in the United States at the time of the commission of the unlawful act giving rise to forfeiture and has become and is forfeitable to the United States.

WHEREFORE, the United States of America respectfully prays the Court that:

1. Due notice be given to all parties to appear and show cause why the forfeiture should not be decreed;
2. Judgment be entered declaring the TARGET USDC to be condemned and forfeited to the United States of America for disposition according to law; and
3. The United States be granted such other and further relief as this Court may deem just and proper, together with the costs and disbursements of this action, including but not limited to the expenses of maintenance and protection of the TARGET USDC as required by 28 U.S.C. § 1921.

Respectfully submitted, this the 2nd day of October, 2026.

RUSS FERGUSON
UNITED STATES ATTORNEY

**s/Benjamin Bain-Creed**
FL Bar Number 21436
Assistant United States Attorney
Suite 1650, Carillon Building
227 West Trade Street
Charlotte, North Carolina 28202
Telephone: (704) 344-6222
Facsimile: (704) 344-6629
Email: benjamin.bain-creed@usdoj.gov

STATE OF NORTH CAROLINA
COUNTY OF MECKLENBURG

# VERIFICATION

Courtney Richardson deposes and says under penalty of perjury:

I am a Special Agent with the Federal Bureau of Investigation and one of the agents assigned to this case.

I have read the foregoing Complaint and the factual information contained therein is true according to the best of my knowledge, information, and belief.

Courtney Richardson
Special Agent
Federal Bureau of Investigation