I, Daniel M. Sirmons, Special Agent for the United States Federal Bureau of Investigation, being duly sworn, depose and says:

INTRODUCTION AND AGENT BACKGROUND

1. I am employed as a Special Agent with the Federal Bureau of Investigation ("FBI"), and have been employed in this capacity since February of 1995. I am currently assigned to the FBI Tampa Field Office in Tampa, Florida. I earned a Bachelor of Science in Electrical Engineering from the University of South Florida in 1988. I have attended over 500 hours of training in various aspects of criminal investigations and cyber-related technical training. In my capacity as a Special Agent with the FBI, I have conducted investigations into both criminal and national security matters, focusing on violent crime, narcotics, counterterrorism, counterintelligence, computer intrusions, and cybercrimes to include those involving cryptocurrency to facilitate wire fraud, computer fraud, mail fraud, and money laundering. I have also assisted in the execution of numerous search warrants, resulting in the seizure of paper, electronic, and other forms of evidence.

2. As a Special Agent with the FBI, I have received significant training on how people use computers to commit crimes and the law enforcement techniques that can be utilized to investigate and disrupt such activity. I have also been involved in, among other things, online and in-person undercover operations, as well as controlled drug deliveries and transactions. Moreover, in the course of my investigations and other cases on which I have worked, I have gained experience executing search warrants for physical premises, as well as for electronic evidence, such as the content

and other data associated with email, messenger, financial, and digital-marketplace accounts operating on both the traditional Internet and the dark web.

3. This affidavit is based upon my personal knowledge, my review of documents and other evidence, my conversations with other law enforcement personnel, and my training and experience concerning the use of computers in criminal activity and the forensic analysis of electronically stored information. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

PURPOSE OF AFFIDAVIT

4. This affidavit is submitted in support of an application for a combined criminal and civil seizure warrant for all funds in any form, including Bitcoin or any other cryptocurrency or fiat (the SUBJECT ASSETS) stored in or accessible via the account at Binance Holdings Limited, bearing User ID 39177039 and associated with the email address tanyaglushko99@gmail.com (the TARGET BINANCE ACCOUNT). As set forth below, I submit that there is probable cause to believe that the SUBJECT ASSETS are property constituting, or derived from, proceeds obtained, directly or indirectly, as a result of violations of 18 U.S.C. § 1030, and are, therefore, subject to civil forfeiture by the United States pursuant to 18 U.S.C. § 981(a)(1)(C) and criminal forfeiture pursuant to 18 U.S.C. § 982(a)(2)(B).

5. Additionally, I submit that there is probable cause to believe that the SUBJECT ASSETS constitute property involved in transactions or attempted transactions in violation of 18 U.S.C. § 1956, or are traceable to such property and are, therefore, subject to civil forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A) and criminal forfeiture pursuant to 18 U.S.C. § 982(a)(1).

FORFEITURE AND SEIZURE AUTHORITY

6. The Court's authority to order civil forfeiture of proceeds of violations of 18 U.S.C. § 1030 is found in 18 U.S.C. § 981(a)(1)(C). Section 981(a)(1)(C) provides for the civil forfeiture of any property which constitutes or is derived from proceeds from a violation of, among others, 18 U.S.C. § 1030. The Court's authority to order criminal forfeiture of proceeds of violations of 18 U.S.C. § 1030 is found in 18 U.S.C. § 982(a)(2).

7. The Court's authority to order civil forfeiture of property for violations of 18 U.S.C. § 1956 is found in 18 U.S.C. § 981(a)(1)(A). Section 981(a)(1)(A) authorizes the forfeiture of all property involved in a transaction in violation of 18 U.S.C. § 1956. The Court's authority to order criminal forfeiture of property for violations of 18 U.S.C. § 1956 is found in 18 U.S.C. § 982(a)(1), which authorizes the forfeiture of any property involved in a violation of 18 U.S.C. § 1956.

8. Civil seizure warrants are authorized by 18 U.S.C. § 981(b)(1). Section 981(b)(3) provides that seizure warrants may be issued by a judicial officer "in any district in which a forfeiture action against the property may be filed . . . and may be executed in any district in which the property is found . . . ."

9. Criminal seizure warrants are authorized by 21 U.S.C. § 853(f), as incorporated by 18 U.S.C. § 982(b)(1). Section 853(f) specifically provides that a court may issue a criminal seizure warrant when it "determines that there is probable cause to believe that the property to be seized would, in the event of conviction, be subject to forfeiture and that a protective order under 21 U.S.C. § 853(e) may not be sufficient to assure the availability of the property for forfeiture." As set forth further below, there is a substantial risk that the SUBJECT ASSETS will be withdrawn, moved, dissipated, or otherwise become unavailable for forfeiture unless they are seized and removed from the TARGET BINANCE ACCOUNT. As cryptocurrencies, the SUBJECT ASSETS are inherently portable and fungible. Binance Holdings Limited ("Binance") claims that it is a non-U.S. company and, therefore, is not subject to U.S. jurisdiction and cannot be compelled by U.S. process. Binance has further indicated, however, that it is willing to place a temporary hold if provided with a seizure warrant in order to allow the United States time to formally execute the warrant pursuant to the terms of our countries' mutual legal assistance treaty and the applicable laws of the Cayman Islands, which is where Binance is registered. Binance has also indicated that it will not keep an account, like the TARGET BINANCE ACCOUNT, locked for an indefinite period of time without providing notification and some reasoning to the account holder, which could compromise this ongoing criminal investigation. I therefore submit that a protective order under 21 U.S.C. § 853(e) would not be sufficient to assure that the SUBJECT ASSETS will remain available for forfeiture.

10. This Court has the authority to issue seizure warrants for assets located in a foreign jurisdiction pursuant to 18 U.S.C. § 981(b)(3). Section 981(b)(3) provides that a seizure warrant may be issued by a "judicial officer in any district in which a forfeiture action against the property may be filed under [28 U.S.C. § 1355(b)], and may be executed in any district in which the property is found, or transmitted to the central authority of any foreign state for service in accordance with any treaty or other international agreement." 18 U.S.C. § 981(b)(3). Pursuant to 28 U.S.C. § 1355(b), a forfeiture action may be brought in any district court where any of the acts giving rise to the forfeiture occurred, even as to property located in a foreign jurisdiction.

BACKGROUND ON CRYPTOCURRENCIES AND TRANSACTION ANALYSIS

11. Bitcoin[1] is a type of virtual currency, circulated over the Internet. Bitcoin are not issued by any government, bank, or company, but rather are controlled through computer software operating via a decentralized, peer-to-peer network.

12. Bitcoin can be exchanged directly, person to person, through a cryptocurrency exchange, or through other intermediaries. Bitcoin are sent and received from Bitcoin "addresses." A Bitcoin address is somewhat analogous to a bank account number and is represented as a 26-to-35-character-long case-sensitive string of letters and numbers. Each Bitcoin address is controlled through the use of a unique

[1] Since Bitcoin is both a currency and a protocol, capitalization differs. Accepted practice is to use "Bitcoin" (singular with an uppercase letter B) to label the protocol, software, and community, and "bitcoin" (with a lowercase letter b) to label units of the currency. That practice is adopted here.

corresponding private key. This key is the cryptographic equivalent of a password, or pin, and is necessary to access the Bitcoin address. Only the holder of an address's private key can authorize any transfers of bitcoin from that address to other Bitcoin addresses. The individual or entity who holds the private key for a Bitcoin address is therefore considered the "owner" of the address. Users can operate multiple Bitcoin addresses at any given time and may use a unique Bitcoin address for each and every transaction. Users often combine multiple Bitcoin addresses (and their corresponding private keys) in a single logical unit known as a Bitcoin "wallet."

13. Although cryptocurrencies such as Bitcoin have legitimate uses, cryptocurrency is often used by individuals and organizations for criminal purposes, such as money laundering. By maintaining multiple wallets, those who use cryptocurrency for illicit purposes can attempt to thwart law enforcement's efforts to track proceeds of illicit activities. Although it's not completely anonymous, Bitcoin allows users to transfer funds more anonymously than would be possible through traditional banking and financial systems.

14. While a Bitcoin address itself does not generally reveal the address's owner (unless the owner opts to make information about the owner's Bitcoin address publicly available), the Bitcoin blockchain is an open, distributed ledger that records transactions of bitcoin between two addresses efficiently and in a verifiable and permanent way. Investigators can sometimes use the blockchain to identify the owner of a particular Bitcoin address or identify Bitcoin addresses that likely all belong to the same owner. For example, because the blockchain serves as a searchable public ledger

of every Bitcoin transaction, investigators can trace transactions to other Bitcoin addresses, including Bitcoin exchanges and Bitcoin payment processors.

15. Investigators may cluster Bitcoin addresses believed to be held by the same owner for the purposes of blockchain analysis into a single "merge wallet." Two ways that analysts determine that multiple addresses are likely under the control of the same owner are called "co-spending" and "change address analysis." "Co-spending" is when a number of Bitcoin addresses are all used to send bitcoin in a single transaction. This indicates that a single owner holds the private keys for all those addresses. "Change address analysis" identifies addresses operating as "change addresses" for a particular account owner. Each bitcoin transaction requires that all the bitcoin at a given address be sent to new addresses. If the owner of the bitcoin wants to spend less than the complete amount of bitcoin held at one of their addresses, they send the excess bitcoin to a new address for which they also hold the private key, called a "change address." Change addresses are therefore likely held by the same owner as the original Bitcoin address.

16. Bitcoin is just one of many varieties of virtual currency. TetherUS, also referred to as Tether, is a cryptocurrency purportedly backed by the United States dollars. Tether was originally designed to always be worth $1, and the company responsible for issuing Tether purportedly maintained $1 in reserves for each Tether issued.

BACKGROUND ON BINANCE

17. Binance Holdings Limited ("Binance"), which is registered in the Cayman Islands, owns and operates Binance.com, a cryptocurrency exchange that provides a platform for trading various cryptocurrencies and exchanging cryptocurrencies for fiat currencies. Binance is one of the largest cryptocurrency exchanges in the world in terms of trading volume. Among other services, Binance provides customers with "custodial wallets," meaning that Binance maintains the private keys relating to the customer's cryptocurrency and therefore has complete control over client funds. Binance offers its services to customers around the world, including the United States.

18. Customers use exchanges like Binance to trade one form of digital currency for another, such as exchanging bitcoin for Tether, or to exchange digital currency into fiat money. In my training, knowledge, and experience, ransomware attackers frequently use cryptocurrency exchanges such as Binance to launder or obfuscate their illicit gains.

STATEMENT OF PROBABLE CAUSE

19. Ransomware is a type of malware that compromises a victim's computer network and threatens to withhold access to and/or publish victim data unless a ransom is paid. Beginning in approximately August 2019, and continuing to the present, victims in the United States and around the world, including within the Middle District of Florida, have been victimized by ransomware identified as "NetWalker." To date, the ransomware has been deployed on dozens of victims,

including municipalities, hospitals, law enforcement and emergency services, school districts, colleges, and universities. NetWalker is capable of not only encrypting victim data and making it inaccessible to the victim, but also stealing victim data. If a victim does not pay the ransom, the stolen data is often published. To date, NetWalker attacks have resulted in the payment of millions of dollars in ransoms. Due to the global scale of these crimes, multiple domestic and foreign law enforcement agencies are conducting parallel investigations of the actors responsible for NetWalker.

20. NetWalker uses a ransomware-as-a-service model, featuring developers and affiliates (collectively, the "NetWalker Actors"). Developers are responsible for creating and updating the ransomware, and making it available to affiliates. Affiliates are responsible for identifying and attacking high-value victims with the ransomware. After a victim pays, developers and affiliates split the ransom.

21. Once a victim's computer network is compromised and the data is encrypted, the NetWalker Actors deliver a file, or ransom note, to the victim. Below, a representative ransom note has been recreated in part:

> Hi! Your files are encrypted by Netwalker . . . If for some reason you read this text before the encryption ended, this can be understood by the fact that the computer slows down, and your heart rate has increased due to the ability to turn it off, then we recommend that you move away from the computer and accept that you have been compromised. Rebooting/shutdown will cause you to lose files without the possibility of recovery . . . Our encryption algorithms are very strong and your files are very well protected, the only way to get your files back is to cooperate with us and get the decrypter program. Do not try to recover your files without a decrypter program, you may damage them and

then they will be impossible to recover. For us this is just business.

22. The ransom note also provides the victim with a unique code and the URL to the NetWalker Actors's Tor website.[2] After entering the code on the website, the NetWalker Actors provide the victim with the amount of ransom demanded and instructions for payment. The NetWalker Actors and victim can communicate directly with one another on the Tor website.

23. The NetWalker Actors commonly gain unauthorized access to a victim's computer network days or weeks prior to the delivery of the ransom note. During this time, the NetWalker Actors surreptitiously elevate their privileges within the network while spreading the ransomware from workstation to workstation. The NetWalker Actors send the ransom note only once they are satisfied that they have sufficiently infiltrated the victim's network to extort payment.

24. In or about May 2020, the NetWalker ransomware was deployed on a U.S. based company ("Victim Company A"). Victim Company A was only able to regain access to its critical data after paying 37.58 bitcoin in ransom, or approximately $353,900.46 on the date of transfer. On May 30, 2020, at 20:15, Coordinated Universal Time (UTC), Victim Company A paid the 37.58 bitcoin ransom to a single bitcoin

[2] The Onion Router ("Tor") is a network of computers distributed around the world designed to conceal the true IP addresses of the network's users. The Tor network also enables websites to operate in a manner that conceals the true IP address of the server hosting the website.

wallet. Analysis of the bitcoin blockchain indicates that approximately 30 minutes later, at 20:44 UTC, this bitcoin wallet sent the entirety of those funds to four bitcoin addresses, including "Merge E" and "Wallet A", in a single transaction. Specifically, 30.07 bitcoin was sent to the group of addresses identified as "Merge E" on Exhibit 1, and 1.88 bitcoin was sent to the address identified as "Wallet A" on Exhibit 1. Based on change address analysis and co-spending, investigators believe that the addresses located at Merge E are controlled by the same owners. Investigators were unable to determine if the two addresses receiving the small, remaining balance of the ransom funds were controlled by the same owners.

25. On or about June 2020, the NetWalker ransomware was deployed on a second U.S. based company ("Victim Company B"). Victim Company B was only able to regain access to its critical data after paying 106.168 bitcoin in ransom, or approximately $999,094.54 on the date of transfer. On June 2, 2020, at 21:23 UTC, Victim Company B paid the 106.168 bitcoin ransom to a single bitcoin wallet. Analysis of the bitcoin blockchain indicates that approximately 30 minutes later, at 21:53 UTC, this bitcoin wallet sent the entirety of those funds to four bitcoin addresses, including Merge E and Wallet A, in a single transaction. Specifically, 89.18 bitcoin was sent to Merge E, and 4.25 bitcoin was sent to Wallet A. Investigators were unable to determine if the two addresses receiving the small, remaining balance of the ransom funds were controlled by the same owners.

26. In or about June 2020, the NetWalker ransomware was deployed on a third U.S. based company ("Victim Company C"). Victim Company C was only able

to regain access to its critical data after paying 303.651 bitcoin in ransom, or approximately $2,860,432.30 on the date of transfer. On June 8, 2020, at 17:27 UTC, Victim Company C paid the 303.651 bitcoin ransom to a single bitcoin wallet. Analysis of the bitcoin blockchain indicates that approximately 30 minutes later, at 17:53 UTC, this bitcoin wallet sent the entirety of those funds to four bitcoin addresses, including Merge E and Wallet A, in a single transaction. Specifically, 255.07 bitcoin was sent to Merge E, and 12.15 bitcoin was sent to Wallet A. Once again, investigators were unable to determine if the two addresses receiving the small, remaining balance of the ransom funds were controlled by the same owners.

27. As described below, from June 6-22, 2020, Merge E and Wallet A engaged in a series of rapid transfers that are consistent with efforts taken to conceal the nature and source of the illicit funds. On June 6, 2020, at 11:59 UTC, Merge E sent two transactions totaling 29.48 bitcoin to a group of addresses identified as "Merge F" on Exhibit 1. Based on change address analysis and co-spending, investigators believe that the addresses located at Merge F are controlled by the same owners. Approximately four hours later, at 14:03 UTC, Merge F sent two transactions totaling 8.89 bitcoin to a group of bitcoin addresses identified as "Merge G" on Exhibit 1. Again, based on change address analysis and co-spending, investigators believe that Merge G is controlled by the same owners.

28. Similarly, on June 11, 2020, at 07:19 UTC, Wallet A sent seven bitcoin to a single address identified as "Wallet B" on Exhibit 1. Approximately seven hours later, at 14:57 UTC, Wallet B sent 4.7 bitcoin to a single address identified as "Wallet

C" on Exhibit 1. On June 22, 2020, at 13:59 UTC, Wallet C sent 1.66 bitcoin to a single address identified as "Wallet D" on Exhibit 1. Approximately ten minutes later, at 14:10 UTC, Wallet D sent 1.48 bitcoin to Merge G.

29. As described above, Merge G was the recipient of ransom payments made by Victim Company A, Victim Company B, and Victim Company C. From June 7-22, 2020, Merge G made three deposits totaling $172,281.22 as of the date of this affidavit directly into the TARGET BINANCE ACCOUNT. On June 7, 2020, at 10:24 UTC, Merge G sent 8.879 bitcoin to the TARGET BINANCE ACCOUNT. On June 22, 2020, at approximately 15:09 UTC, Merge G sent five bitcoin to the TARGET BINANCE ACCOUNT. Minutes later, at 15:15 UTC, Merge G sent an additional 4.4 bitcoin to the TARGET BINANCE ACCOUNT. The anonymity provided by bitcoin, coupled with the series of rapid transfers following the initial transfer of the victim's ransom payments to the NetWalker payment addresses are consistent with efforts taken to conceal the nature and source of the illicit funds.

30. Binance records revealed that the TARGET BINANCE ACCOUNT is registered to a 20-year-old Ukrainian national named Tetiana Lukianiuk. These records indicate that between January 30, 2020, and June 22, 2020, Lukianiuk exchanged the majority of bitcoin in the TARGET BINANCE ACCOUNT for Tether. As of June 25, 2020, the TARGET BINANCE ACCOUNT held two cryptocurrency assets, bitcoin and Tether, currently valued at approximately $433,271.39.

CONCLUSION

31. Based on all of the foregoing, as well as my training, education, and experience, I submit that there is probable cause to believe that the SUBJECT ASSETS are proceeds of violations of, *inter alia*, 18 U.S.C. § 1030—specifically, the attacks on the three Victim Companies occurring in May and June 2020, and are, therefore, subject to civil forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C) and criminal forfeiture pursuant to 18 U.S.C. § 982(a)(2)(B). Additionally, there is probable cause to believe that the SUBJECT ASSETS constitute property involved in money laundering, in violation of 18 U.S.C. § 1956, and are, therefore, subject to civil forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A) and criminal forfeiture pursuant to 18 U.S.C. § 982(a)(1).

Daniel M. Sirmons

DANIEL M. SIRMONS
FBI SPECIAL AGENT

Affidavit submitted by email and attested to me as true and accurate by videoconference consistent with Fed.R.Crim. P. 41(d)(3), as incorporated by 18 U.S.C. § 981(b)(2), before me on July 10, 2020.

Amanda A. Sansone

AMANDA A. SANSONE
UNITED STATES MAGISTRATE JUDGE

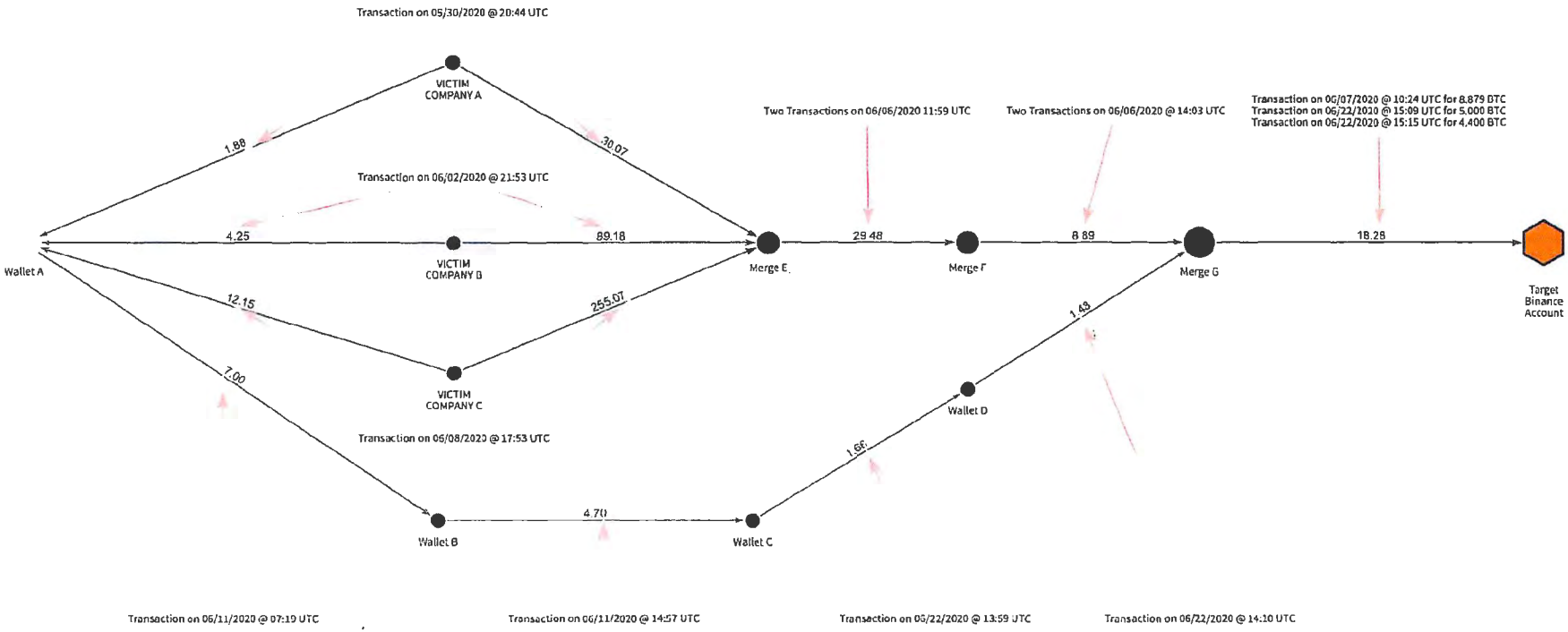
Transaction on 05/30/2020 @ 20:44 UTC
VICTIM COMPANY A
1.88
30.07
Transaction on 06/02/2020 @ 21:53 UTC
4.25
89.18
VICTIM COMPANY B
Wallet A
12.15
255.07
VICTIM COMPANY C
7.00
Transaction on 06/08/2020 @ 17:53 UTC
Wallet B
4.70
Wallet C
1.66
Wallet D
1.49
Two Transactions on 06/06/2020 11:59 UTC
29.48
Merge E
Two Transactions on 06/06/2020 @ 14:03 UTC
8.89
Merge F
Transaction on 06/07/2020 @ 10:24 UTC for 8.879 BTC
Transaction on 06/22/2020 @ 15:09 UTC for 5.000 BTC
Transaction on 06/22/2020 @ 15:15 UTC for 4.400 BTC
18.28
Merge G
Target Binance Account
Transaction on 06/11/2020 @ 07:19 UTC
Transaction on 06/11/2020 @ 14:57 UTC
Transaction on 06/22/2020 @ 13:59 UTC
Transaction on 06/22/2020 @ 14:10 UTC

EXHIBIT 1