ATTACHMENT A

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

UNITED STATES OF AMERICA **v.** **OLAKITAN OLUWALADE,** **ODUNAYO BABA OLUWALADE,** **and** **KELLY LAMONT WILLIAMS** **Defendants.**	1:21-mj-346 TMD 1:21-mj-347 TMD Case No. 1:21-mj-348 TMD

AFFIDAVIT IN SUPPORT OF
CRIMINAL COMPLAINTS AND ARREST WARRANTS

I, Dennis Senft, being duly sworn, hereby declare as follows:

INTRODUCTION AND AGENT BACKGROUND

1. Your Affiant is a Special Agent with Homeland Security Investigations ("HSI"). As such, I am "an investigative or law enforcement officer of the United States" within the meaning of 18 U.S.C. § 2510(7) and empowered by law to conduct investigations and to make arrests for offenses enumerated in 18 U.S.C. § 2516. Your Affiant has been a Special Agent with HSI since 2007.

2. Your Affiant completed the Federal Criminal Investigator Training Program and the Immigration and Customs Enforcement ("ICE") Special Agent Training at the Federal Law Enforcement Training Center located in Glynco, Georgia. Your Affiant received training in narcotics trafficking, money laundering and other investigations. Your Affiant also received additional training in methods to trace illegal proceeds and prove financial crimes, asset forfeiture, and financial investigations, including but not limited to financial fraud.

3. Your Affiant is currently assigned to the Office of the Special Agent in Charge, Baltimore, Maryland, as well as the High Intensity Drug Trafficking Area (HIDTA), Illicit Online Market Initiative (IOMI), a component of the HSI Baltimore Transnational Cyber Crimes Team (TCCT), where I am tasked with investigating criminal activity that is facilitated through the use of the internet the dark web and digital currencies. Prior to this assignment I was assigned to the HSI Baltimore HIDTA, Drug and Money Laundering Initiative ("DMLI") Task Force in Southern Maryland. This particular Task Force investigates drug and money laundering organizations in the Washington, D.C., and Baltimore, Maryland region. Based on training and experience, your Affiant is familiar with the methods and techniques associated with financial crimes and the organization of money laundering conspiracies. In the course of conducting these investigations, your Affiant has been involved in the use of the following investigative techniques: interviewing informants and cooperating witnesses; conducting physical surveillance; conducting short and long-term undercover operations, including reverse undercover drug operations; consensual monitoring and recording of both telephonic and non-telephonic communications; analyzing telephone pen register and caller identification system data; conducting court-authorized electronic surveillance, including Title III wire interceptions; and preparing and executing search warrants that have led to substantial seizures of narcotics, currency, firearms, devices used in fraud schemes and other contraband. I have participated in and was the case agent for Title III operations, comprised of surveillance operations, monitoring Title III wire interceptions, and analyzing telephone records.

4. I have personally been involved with this investigation since it started in January 2021. I am familiar with the facts and circumstances of this investigation. The facts set forth in this affidavit are based on my own personal knowledge, knowledge obtained from other

individuals during my participation in this investigation, including other law enforcement officers, interviews of witnesses, review of records related to this investigation, communications with others who have knowledge of the events and circumstances described herein, and information gained through my training and experience. Because this affidavit is being submitted for the limited purpose of establishing probable cause in support of the Criminal Complaints and Arrest Warrants, I have not included every fact known to me or to the United States. Unless otherwise indicated, all written and oral statements referred to herein are set forth in substance and in part, rather than verbatim.

5. I make this affidavit in support of a criminal complaint and arrest warrant for each of the individuals listed below. Based on the following facts, there is probable cause to believe that, in the District of Maryland and elsewhere, **OLAKITAN OLUWALADE ("OLAKI"), ODUNAYO BABA OLUWALADE ("BABA"),** and **KELLY LAMONT WILLIAMS ("WILLIAMS")** committed wire fraud conspiracy in violation of 18 U.S.C. § 1349.

BACKGROUND ON COVID-19 AND COMPANY 1'S VACCINE

6. In late 2019, a novel coronavirus, SARS-CoV-2, was first detected in Wuhan, China, causing outbreaks of the disease COVID-19 that have since spread globally. COVID-19 is highly contagious and causes severe acute respiratory syndrome. On March 13, 2020, the President of the United States declared a national emergency due to the COVID-19 pandemic.

7. Company 1 is a biotechnology company based in Cambridge, Massachusetts. The company focuses on drug discovery, drug development, and vaccine technologies, including a vaccine for COVID-19. Company 1 utilizes a website with a URL of www.modernatx.com as their forward facing, public website on the World Wide Web for anyone to obtain information on the products the company has developed, or is in the process of developing, including those

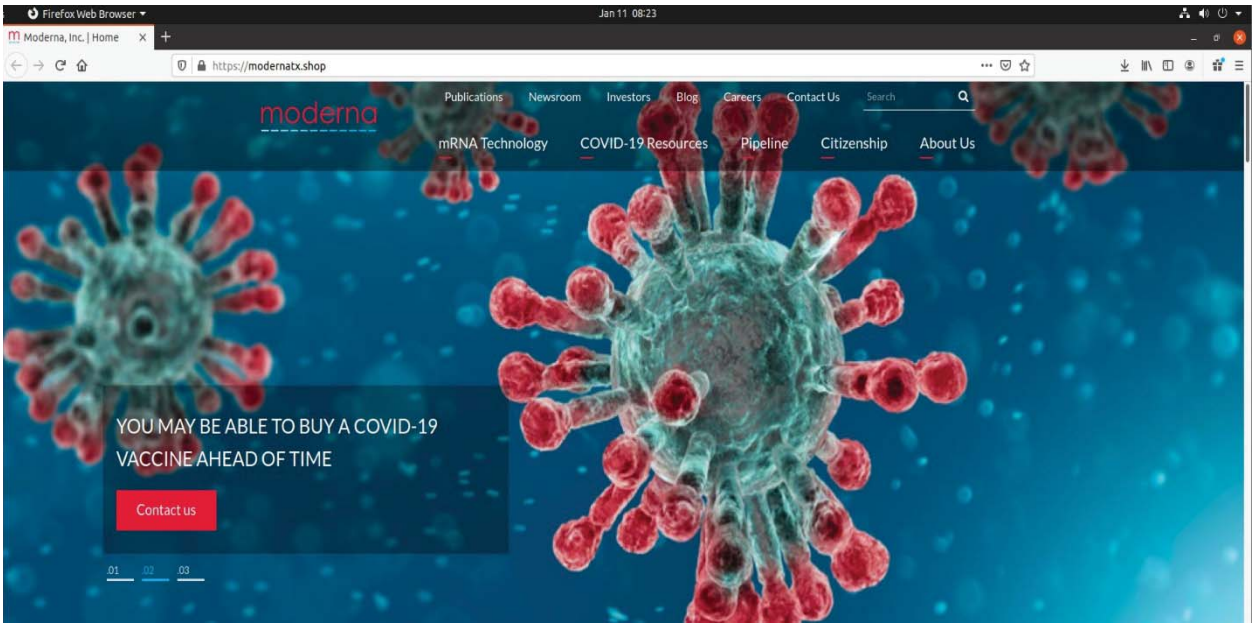
focusing on combating the COVID-19 pandemic. On December 18, 2020 the FDA issued an emergency use authorization for Company 1's COVID-19 vaccine to be distributed in the United States.

THE FRAUDULENT WEBSITE PURPORTING TO SELL COMPANY 1 VACCINES

8. On January 11, 2021, the HSI Intellectual Property Rights Center and the HSI Cyber Crimes Center became aware of a fraudulent replication of Company 1's website, named "Modernatx.shop" (the "Fake Domain"). Publicly available databases indicated that the Fake Domain was registered through NameCheap, Inc., a company with headquarters in Phoenix, Arizona.

9. The home page of the Fake Domain appeared visually similar to Company 1's real website. For example, the Fake Domain displayed the name and trademarked logos for Company 1, and the logo, markings, colors and text on the Fake Domain were visually similar to that of Company 1's actual home page. The source code of the Fake Domain indicated that the creator of the site used a website tool to copy Company 1's actual website in order to create the Fake Domain.

10. However, the Fake Domain (unlike Company 1's home page) had the text: "YOU MAY BE ABLE TO BUY A COVID-19 VACCINE AHEAD OF TIME," with a link to "Contact us." A screenshot of the domain on or about January 11, 2021 appears below:



UNDERCOVER PURCHASE

11. On or about January 11, 2021, at approximately 3:58 p.m., an HSI Special Agent, in an undercover capacity ("UC"), contacted a number listed on the Fake Domain, which investigators determined was linked to a WhatsApp account. The WhatsApp number replied at approximately 5:53 p.m. requesting an email address to contact the UC, and the UC provided an email contact at approximately 6:02 p.m.

12. Approximately four minutes later the UC received an email, at the address the UC had provided, from sales@modernatx.shop, an email address which appears on the "Contact Us" page of the Fake Domain. The email purported to welcome the UC to Company 1 and provided a brief description of Company 1 and the storage requirements of Company 1's vaccine.

13. After several additional emails, the UC received information regarding payment, delivery, and purchase for alleged Company 1 vaccines from a Google email address.[1] The UC was sent a purported invoice for 200 doses of Company 1's vaccine at $30.00 (USD) per dose, for

[1] IP Login information obtained by the government indicates that this address was logged into from Cameroon.

a total of $6,000. The payment terms were listed as 50% up front and 50% upon delivery.

14. The UC was instructed to send payment to a Navy Federal Credit Union account in the name of **KELLY LAMONT WILLIAMS.** The UC transferred a portion of the funds to **WILLIAMS**'s account as directed.

15. On January 14, 2021, Magistrate Judge Thomas M. DiGirolamo authorized the seizure of the Fake Domain, and the government subsequently seized the Fake Domain. *See* 21-MJ-110-TMD.

OLAKI, BABA, AND WILLIAMS'S DISCUSS THE SCHEME

16. On January 15, 2021, HSI Agents executed a search warrant at **WILLIAMS**'s home. *See* 21-MJ-109-TMD. On January 25, 2021, HSI executed search warrants at **OLAKI** and **BABA**'s homes. *See* 21-mj-169-TMD, 21-mj-170-TMD. As a result of these searches, investigators recovered a number of communications between **BABA**, **OLAKI**, and **WILLIAMS** discussing the fraud scheme:[2]

17. On or about November 16, 2020, **WILLIAMS** and **OLAKI** texted as follows:

> **OLAKI**: Yo bro. Tbh, this my cousin's[3] jug.[4] He say the bank account gonna b straight after the jug tho. It's 1,600 per week until he can't push it no more. Y'all split it."
>
> **WILLIAMS**: Ard bet, what he doing tho droppin check in it? Like whats the jug Im with it tho.

[2] In addition to those texts detailed below, investigators also discovered text messages between **OLAKI** and **BABA** in or about June 30, 2020 discussing how to create a fraudulent application for COVID-19 Economic Injury Disaster Loans (EIDL). **OLAKI** instructed BABA that he was, "putting $150000 revenue $135000 cogs. . . on the EIDL shit. Make sure you put 5-10 employees. That's really it. I just did one . . . I used [someone else's] social . . . if you put you have employees they give you $1k each. That doesn't have to get paid back."

[3] Investigators have determined that **BABA** and **OLAKI** are cousins.

[4] A review of **OLAKI**'s phone indicates that he repeatedly used the term "jug" to refer to potential illegal activity. For example, on or about July 18, 2020, **OLAKI** texted another individual about a "quick jug that I need help with. It's some simple shit and I'll break you off like 2-3k."

18. At or about that same day, **OLAKI** texted **BABA**, "I got a nigga with Navy fed."

BABA sent **OLAKI** back a message saying "Awww shit," followed by:

Bank name
Account name (plus middle)
Address
A Number
R number
Bank address
Email addy
Login
That's the info he gon need but I'm boutta hit my mans up now and let him know

19. On or about November 16, **OLAKI** sent the requested information to **WILLIAMS**, writing:

OLAKI: Nothing gonna happen to your bank account[.] Nay Fed is sweet.

WILLIAMS: Bet. Wassup.

OLAKI: All you gotta do is fill out a form And send it back to me. I'll keep you updated on what's going on.

Bank name
Account name (plus middle)
Address
Acct number
Bank address
Email address
Password

Change your password then send it. Also. Since I'm the middleman. Imma take 20% of your cut if that's cool. You're supposed to get like 15-30k.

WILLIAMS: Bet.

20. **WILLIAMS** provided his banking information to **OLAKI**, and **OLAKI** then forwarded **WILLIAMS**'s bank information to **BABA** on November 17, 2020.

21. On or about November 25, 2020, **OLAKI** texted **WILLIAMS**, "Yo what's your PIN to your Navy fed acccount?" **WILLIAMS** sent back his pin to **OLAKI**.

22. Later that day, **OLAKI** wrote, "They were gonna put 16k on it but they said they're gonna try to get a bigger slip like 30-40k. That's why no money has hit yet. And the bank account not really supposed to close."

23. On or about December 1, 2020, **OLAKI** sent **WILLIAMS** a screen capture of a text message conversation from **BABA**. **BABA** wrote: "Yoo they said they tried to send the bread to Kelly shit but that shit wasn't accepting it. Maybe it's cause it's shit not that old fr but he told me boutta get another transfer and try again with his account then he said if it don't work they prolly can't."

24. On January 15, 2021, investigators used **WILLIAMS**'s phone to send **BABA** a message: "Yo where u want me send the bread?" (referring to the cash investigators had sent to **WILLIAMS**'s bank account for the purchase of alleged vaccines as directed). **BABA** replied, "Yea send me some thru zelle and some through cash app." Both Zelle & Cash App are online payment platforms. **BABA** provided his Cash App User ID name, and investigators made a cash transfer of the funds to **BABA's** Cash App account per his request.

[redacted]

25. As discussed above investigators executed search warrants at **OLAKI, BABA,** and **WILLIAMS's** residence.

26. [redacted]

27. [redacted]

28. [redacted]

CONCLUSION

29. Based on the information set forth in this affidavit, I respectfully submit there is probable cause that **OLAKITAN OLUWALADE**, **ODUNAYO BABA OLUWALADE**, and **KELLY LAMONT WILLIAMS** committing the offense of wire fraud conspiracy in violation of 18 U.S.C. § 1349.

DENNIS P SENFT JR Digitally signed by DENNIS P SENFT JR Date: 2021.02.09 12:38:55 -05'00'

Dennis Senft
Special Agent, HSI

Affidavit submitted by email and attested to me as true and accurate by telephone consistent with Fed. R. Crim. P. 4.1 and 4(d) this 10 day of Feb, 2021.

Hon. Thomas M. DiGirolamo
United State Magistrate Judge