

UNITED STATES DISTRICT COURT

for the
District of MinnesotaIN THE MATTER OF THE SEARCH OF A
PERSON LOCATED IN THE DISTRICT OF
MINNESOTA, DESCRIBED IN
ATTACHMENT A, FOR THE ITEMS
DESCRIBED IN ATTACHMENT B

SEALED BY ORDER OF THE COURT

Case No. 22-mj-742 (TNL)

APPLICATION FOR A SEARCH WARRANT

I, J. A. Myszkiewicz, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment A, incorporated here

located in the State and District of Minnesota, there is now concealed:

See Attachment B, incorporated here

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code SectionOffense Description

Title 18, United States Code, Section 1028(a)(7)
Title 18, United States Code, Section 1030(a)(5)(A)
Title 18, United States Code, Section 371

Identity Theft
Intentional Damage to a Protected Computer
Conspiracy to Commit Identity Theft and/or to Cause
Intentional Damage to a Protected Computer

The application is based on these facts:

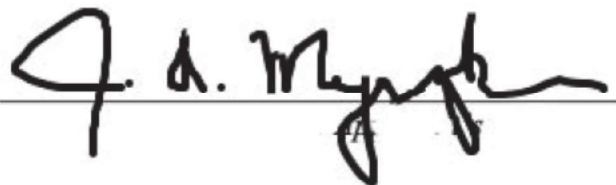
See Affidavit, incorporated here

☒ Continued on the attached sheet.

SUBSCRIBED and SWORN before me by reliable
electronic means (FaceTime, Zoom and/or email)
pursuant to Fed. R. Crim. P. 41(d)(3)

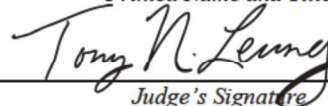
Date: September 7, 2022

City and State: Minneapolis, MN



J. A. Myszkiewicz, Special Agent
Federal Bureau of Investigation

Printed Name and Title



Judge's Signature

The Honorable Tony N. Leung
United States Magistrate Judge

Printed Name and Title

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MINNESOTA

IN THE MATTER OF THE SEARCH OF
A PERSON LOCATED IN THE DISTRICT
OF MINNESOTA, DESCRIBED IN
ATTACHMENT A, FOR THE ITEMS
DESCRIBED IN ATTACHMENT B

Case No. 22-mj-742 (TNL)

AFFIDAVIT IN SUPPORT OF APPLICATION
UNDER RULE 41 FOR WARRANT TO SEARCH AND SEIZE

I, J. A. Myszkiewicz, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the search of the person of Michael Lindell, as described in Attachment A, for the things described in Attachment B, including the cellular telephone assigned call number [REDACTED].

2. I am a Special Agent of the Federal Bureau of Investigation (FBI) currently assigned to the Denver Division. As such, I am an investigative or law enforcement agent of the United States authorized under Title 18, United States Code, Section 3052, that is, an officer of the United States who is empowered by law to conduct investigations, to make arrests, and to collect evidence for various violations of federal law. I have been employed as a Special Agent of the FBI since August 2007.

3. I have experience in conducting investigations involving cyber-related matters, financial fraud, and other violations of federal law. Through my experience and training, I have become familiar with activities of individuals engaged in illegal activities, to include their techniques, methods, language, and terms. During my career, I have been involved in investigations that have included the use of various surveillance techniques and the execution of

numerous search and seizure warrants. In my career with the FBI, I have received continual digital forensics training and am experienced in the identification, acquisition, duplication, examination, and analysis of digital evidence. I maintain industry-standard cyber security certifications as an incident handler, intrusion analyst, forensic analyst, and ethical hacker. I am currently assigned to the FBI Denver Division Cyber Crimes Squad, wherein my primary duties and responsibilities include the investigation of criminal violations relating to unauthorized access into protected computer systems, in violation of Title 18 United States Code, Section 1030, and fraud and related activity in connection with access devices, in violation of Title 18 United States Code, Section 1029.

4. The facts in this application derive principally from emails and documents voluntarily obtained from Mesa County, Colorado; interviews with (and records obtained from) witnesses from the Mesa County Clerk and Recorder's Office, the Colorado Secretary of State's Office, and Dominion Voting Systems; records obtained by court order from various telecommunications and technology companies; and conversations with law enforcement officers involved in this investigation. Because this application is being submitted for the limited purpose of obtaining a search warrant for a particular electronic device, I have not set forth every fact learned by the government during this investigation.

5. All of the dates identified in this affidavit are approximate, reflecting the date "on or about" events occurred. All times identified in this affidavit are approximate and generally reflect "Mountain Time," unless otherwise stated. For example, some times described below appear as UTC (Coordinated Universal Time), which is either six or seven hours ahead of Mountain Time (depending on daylight savings time). All transcriptions of dialogue on audio or

video recordings are unofficial, and were completed by FBI personnel using their best efforts to discern the exact wording used.

6. 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 violations of 18 U.S.C. §§ 1028(a)(7) (identity theft), 1030(a)(5)(A) (intentional damage to a protected computer), and 371 (conspiracy to commit identity theft and/or to cause intentional damage to a protected computer)—together, the “SUBJECT OFFENSES”—have been committed by [REDACTED], [REDACTED], Michael Lindell, and [REDACTED], among other co-conspirators known and unknown to the government (the “SUBJECTS”). There is also probable cause to seize and search the cellular devices of [REDACTED], Michael Lindell, and [REDACTED].

7. This affidavit is submitted in support of an application to search the person of Michael Lindell, described in Attachment A, for the items described in Attachment B, including the cellular telephone assigned call number [REDACTED] (the “Lindell Cellphone”). The United States is seeking separate warrants to seize and search [REDACTED], likely in the [REDACTED] and the [REDACTED], respectively, although those Districts are subject to change. For instance, the warrant for [REDACTED] may be sought in the [REDACTED].

8. On August 31, 2022, I obtained warrants for the search and seizure of historical and prospective location information related to the Lindell Cellphone and the [REDACTED]. These warrants were issued in the District of Colorado by U.S. Magistrate Judge James P. O’Hara. According to the location information reported by Verizon Wireless related to the

Lindell Cellphone, the Lindell Cellphone is currently located in the District of Minnesota. Because individuals are typically in close proximity to their cellphones at most times of the day and night, I believe that Michael Lindell is also currently located in the District of Minnesota.

BACKGROUND ON THE COMPUTER FRAUD AND ABUSE ACT

9. 18 U.S.C. § 1030(a)(5)(A) prohibits “knowingly caus[ing] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally caus[ing] damage without authorization, to a protected computer.”

10. “Damage” is defined as “any impairment to the integrity or availability of data, a program, a system, or information.” 18 U.S.C. § 1030(e)(8).

11. A “protected computer,” as relevant here, is (1) a computer “which is used in or affecting interstate or foreign commerce or communication” or (2) a computer that is “part of a voting system” and that (a) is “used for the management, support, or administration of a Federal election” or (b) “has moved in or otherwise affects interstate or foreign commerce.” 18 U.S.C. § 1030(e)(2).

BACKGROUND ON IDENTITY THEFT

12. In pertinent part, 18 U.S.C. § 1028(a)(7) prohibits the unlawful use, transfer, or possession of a “means of identification” of another person “with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.” 18 U.S.C. § 1028(a)(7). As relevant here, the use, transfer, or possession must be in or must affect interstate commerce. *Id.* § 1028(c)(3)(A).

13. Under Colorado law, it is a felony to “attempt[] to influence any public servant by means of deceit . . . with the intent thereby to alter or affect the public servant’s decision, vote,

opinion, or action concerning any matter which is to be considered or performed by him or the agency or body of which he is a member.” Colorado Rev. Stat. § 18-8-306.

PROBABLE CAUSE

A. Introduction

14. In or around April 2021, the Colorado Secretary of State—charged under state law with supervising state elections—began working with County Clerk and Recorders across the state to upgrade the counties’ electronic voting systems. The vast majority of Colorado counties—including Mesa County—lease electronic voting hardware and software from Dominion Voting Systems (Dominion), a private Colorado-based election technology company. The upgrade—called a “Trusted Build”—for Mesa County, Colorado, was scheduled for late May 2021. [REDACTED]

[REDACTED] was to be the principal county representative at the upgrade. Both before and after the upgrade, [REDACTED] has claimed that electronic voting machines are vulnerable to manipulation.

15. Both before and after the May 2021 upgrade, [REDACTED] directed a surreptitious effort to electronically image (that is, copy) Mesa County’s Dominion computer voting machine (CVM). Before the upgrade, [REDACTED] ordered that cameras in the Clerk’s Office be disabled. Separately, Clerk’s Office employees pretextually obtained office access credentials (including to secure elections areas) for a local software engineer named [REDACTED] by providing contradictory and inconsistent explanations regarding [REDACTED] employment relationship with Mesa County to both Colorado Secretary of State officials and Mesa County officials. Following the upgrade, pre- and

post-upgrade CVM images were posted on the Internet, along with videos and photos taken during the installation of the upgrade.

16. [REDACTED] actions were preceded by a visit to Mesa County in April 2021 by [REDACTED] an advocate of theories related to the 2020 presidential election (including the theory that Dominion voting machines were subject to manipulation by outside actors and that the 2020 presidential election results were marred by widespread fraud). As discussed in greater detail below, [REDACTED] offered to assist [REDACTED] in conducting a forensic examination of Mesa County's voting systems without involvement from the Secretary of State or any other arm of Colorado state or local government.

17. The leak of the CVM images, as well as of the videos and photographs of the upgrade, triggered local, state, and federal investigations. The Colorado Secretary of State's Office ultimately de-certified the Mesa County CVM because it could not establish confidence in the "integrity or security" of the machine. Local officials also executed multiple search warrants at the Mesa County Clerk and Recorder's Office and seized additional electronic devices.

18. Subsequent investigation, detailed below, has led investigators to believe that [REDACTED] and other individuals only pretextually obtained access credentials for [REDACTED]. Their true purpose was to provide [REDACTED] credentials to [REDACTED], who would pose as [REDACTED] and use [REDACTED] credentials. The apparent intent was to obtain access to the CVM—and the Trusted Build itself—for [REDACTED] without alerting Colorado Secretary of State officials or Mesa County officials outside the Clerk and Recorder's Office to the presence of an outside actor not employed by Mesa County or the State of Colorado.

19. Further investigation of [REDACTED] activities following the leak of the CVM images revealed that [REDACTED] was likely also involved in an incident related to the Lake County, Ohio,

computer network. Moreover, a review of [REDACTED] financial records and communications records indicated that [REDACTED] communicated extensively with MyPillow Inc. (MyPillow) Chief Executive Officer Michael Lindell throughout 2021, including during key time periods relevant to the events in Mesa County, and that [REDACTED] received hundreds of thousands of dollars in payments from Lindell during this time period. As discussed below, Lindell himself has been active in advancing theories related to the 2020 presidential election (including theories related to the manipulation of Dominion voting machines, such as those in use in Mesa County).

20. The government here seeks authority to seize and search the cellular telephone of Michael Lindell, assigned call number [REDACTED]. As discussed above, the government is separately seeking authority to seize and search [REDACTED] [REDACTED] in the [REDACTED], respectively (or other Districts, as explained previously). A table of the three cellphones sought by these warrants is set forth below:

<u>Telephone Number</u>	<u>Listed Subscriber</u>	<u>Source of Information</u>	<u>Device Information</u>
[REDACTED]	[REDACTED]	Verizon Wireless records (most recently updated June 28, 2022)	IMEI [REDACTED] (effective 3/28/16) IMEI [REDACTED] (effective 6/10/21)
[REDACTED]	[REDACTED]	T-Mobile US records (most recently updated June 28, 2022)	IMEI [REDACTED] (effective 11/18/20)
[REDACTED] (the “Lindell Cellphone”)	My Pillow Inc Chaska, Minnesota Contact name: Mike Lindell ²	Verizon Wireless records (most recently updated June 28, 2022)	IMEI [REDACTED] (effective 12/22/20) IMEI [REDACTED] (effective 8/18/21)

B. Description of [REDACTED] and Lindell

21. [REDACTED] gained Michael Lindell’s attention starting in or around February 2021 for his theory about how the 2020 election was marred by systemic and widespread fraud. [REDACTED] has asserted that election officials have deliberately inflated voter registration rolls in every county in the United States, resulting in “phantom ballots” being generated to rig elections. According to [REDACTED] election officials monitor the returns in an election and inject these “phantom ballots” when necessary to ensure some fixed, predetermined election result. [REDACTED]

² Records received from Apple dated April 7, 2022, indicate that the Lindell Cellphone is the telephone number associated with the iCloud account connected to the email address [REDACTED]. In this same set of Apple records, the Lindell Cellphone is also listed as the telephone number associated with a Mastercard used to make payments for purchases associated with this account. The most recent purchase reflected in these records, using this Mastercard, is a purchase of “MLB Audio Yearly.”

[REDACTED] In the film, [REDACTED] described his theory about widespread election fraud and his discovery of an algorithm that he said proved his theory.

22. Investigators have contacted and interviewed several experienced, county-level government and election officials and staff throughout Colorado during the investigation into this matter. Some of those who were aware of ██████ assertions reported they either recognized upfront that the data ██████ was using as the basis of his theory was not accurate or correct, or they investigated ██████ claims of fraud in their county due to pressures applied from ██████ supporters, such as ██████ (a local political activist and the former campaign manager of a now-member of the U.S. House of Representatives) and ██████

██████████). Not one person contacted was able to verify or corroborate any aspect of ██████████ theory or his claims of widespread election fraud in Colorado. Despite repeated requests from county-level government and election officials and staff, neither ██████████ nor any of his supporters have been able to identify even a single “phantom voter” or “phantom ballot” that was cast in Colorado in the 2020 Elections.

23.

As discussed elsewhere in this affidavit, [REDACTED] was identified by name as an individual involved in receiving information on a hard drive from Mesa County voting machines. [REDACTED]

. According

to a phone interview conducted by the [REDACTED] and described in this article, [REDACTED] confirmed, in substance, that he attended the [REDACTED].³

Michael Lindell

24. Michael “Mike” J. Lindell is a resident of Minnesota where he owns the company MyPillow. Lindell has persistently made public statements regarding purportedly widespread election fraud during the 2020 presidential election. Particularly, Lindell has promoted claims that Dominion election computers were deliberately designed to rig the results of the election. On February 22, 2021, Dominion filed a \$1.3 billion dollar defamation lawsuit in the United States District Court for the District of Columbia that accused Lindell of seeking to boost pillow sales for MyPillow through what Dominion described to be Lindell’s promotion of false claims. *See* Case No. 1:21-CV-445 (D.D.C.), ECF No. 1 (Complaint). In May 2022, Lindell purportedly informed one newspaper that he had “spent about \$30M to retain about 70 lawyers, cyber consultants, private investigators and other staffers for his projects to prove widespread fraud in the 2020 elections.”⁴

25. Between August 10 and 12, 2021, Lindell hosted what he referred to as a “Cyber Symposium” in Sioux Falls, South Dakota. Lindell had promoted the event for months, saying that he would be releasing digital evidence, including computer network traffic, that would demonstrate how voting machines across the United States were hacked by malicious actors, who then used that access to manipulate the results of the 2020 presidential election. The event was broadcast live by several media outlets and video of the event remains widely available on the Internet.

³ [REDACTED]

⁴ *See* <https://www.theguardian.com/us-news/2022/may/12/mike-lindell-trump-election-big-lie>.

C. Mike Lindell Began Communicating with [REDACTED] in February 2021

26. Investigators collected account and communications records from Verizon Wireless for telephone number [REDACTED] (with Mike Lindell listed as the “contact name” from December 16, 2015, to at least June 28, 2022, which is the date of the most current records possessed by the United States) (the “Lindell Cellphone”) and T-Mobile US, Inc. for telephone number [REDACTED] (subscribed to [REDACTED] from December 12, 2019, to at least June 28, 2022, which is the date of the most current records possessed by the United States) (the [REDACTED]). The communications records obtained covered the period from October 2020 to June 28, 2022. No communications were identified between Lindell and [REDACTED] prior to February 22, 2021, the day that Dominion filed its \$1.3 billion dollar defamation lawsuit against Lindell. The first identified communications between Lindell and [REDACTED] occurred two days later, on February 24, 2021:

Date/Time	From	To	Communication
2021-02-24 16:51:46 UTC	[REDACTED]	Lindell Cellphone	Voice (3 min 17 sec)
2021-02-24 18:25:52 UTC	Lindell Cellphone	[REDACTED]	Voice (50 min 8 sec)
2021-02-24 23:25:01 UTC	Lindell Cellphone	[REDACTED]	Voice (19 min 50 sec)
2021-02-24 23:54:50 UTC	Lindell Cellphone	[REDACTED]	Voice (15 min 54 sec)

D. The Mesa County Elections Office

27. [REDACTED]

[REDACTED] The office is located at 200 South Spruce Street, Grand Junction, Colorado 81501, inside of a multi-purpose county building. Within the office—according to Clerk’s Office employees and 21st Judicial District Attorney’s Office investigators who have visited the office—is a dedicated room known as the “Tabulation Room,” where a specialized CVM and other electronics are securely stored and used

to tally voter ballots during elections in Mesa County. The CVM in the Tabulation Room included a server and eight computers connected to that server.

28. The Mesa County CVM is owned by Dominion and leased to Mesa County.⁵ In particular, the leased CVM includes a server connected to eight computers, proprietary software called the Democracy Suite Election Management System, and third-party hardware required to operate Dominion computers. According to Dominion personnel and Secretary of State officials, the CVM is a “closed” system, meaning it is configured to have no Internet access or Wi-Fi access (in order to protect the system from outside interference). Periodic upgrades to the CVM are referred to as “Trusted Builds,” which require the cooperation of Dominion, Mesa County, and the Colorado Secretary of State’s Office.

29. Dominion personnel and Secretary of State officials have described the Trusted Build process to investigators. On the day of a Trusted Build, representatives from each entity come together in-person. According to procedures established by Dominion, the Colorado Secretary of State (not county officials) is responsible for setting BIOS passwords.⁶ Colorado Secretary of State representatives enter the BIOS password to begin the Trusted Build process. Next, Dominion representatives check the now-unlocked BIOS configurations of the CVM equipment to verify that the settings are correct. Colorado Secretary of State representatives then begin to apply the new Trusted Build image to the CVM equipment. Dominion representatives again verify settings and configurations. A few rounds of this process may repeat until the Trusted

⁵ Dominion generates revenue by selling voting technology, licensing software, and providing related services across the United States.

⁶ The “BIOS” is a set of computer routines that enable a computer to start the operating system for the CVM equipment. The BIOS is described in further detail below.

Build upgrade process is completed. Finally, Mesa County representatives are directed to change the passwords for the Windows user accounts on the CVM equipment to passwords known only to Mesa County officials.

30. The Dominion-Mesa County agreement—in a list of prohibited acts—states: “The Licensee shall not, without the prior written permission of Licensor: ... [t]ransfer or copy onto any other storage device or hardware or otherwise copy the Software in whole or in part except for purposes of system backup.” In that agreement, the “Licensee” is Mesa County, and the “Licensor” is Dominion.

31. The computers comprising the Mesa County CVM are “protected computers” within the meaning of 18 U.S.C. § 1030(e)(2)(C). According to the Colorado Secretary of State, Mesa County used its CVM during the 2020 election, which included federal candidates on the ballot. Moreover, according to Dominion, parts of the computers associated with that system were manufactured outside the state of Colorado and moved in interstate commerce.

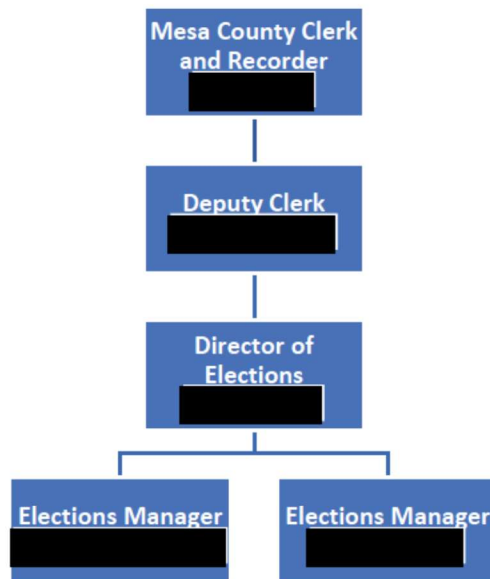
32. According to Mesa County Information Technology (IT) staff, the county building housing the Elections Office maintains a video surveillance system for the Elections Office and Tabulation Room. The surveillance system is used for both routine security and to help ensure a fair, proper election process. Some critical camera angles are directed at the Tabulation Room and the CVM. Camera system maintenance is performed by Mesa County IT staff, and the system has its own server/cloud storage which is separate from all other county camera systems, such as the jail or the sheriff’s office. The retention time of video storage for this camera system is several months, far longer than other county video storage systems.

33. According to 21st Judicial District Attorney’s Office investigators, the county building (including the Elections Office) is also equipped with electronic access controls for

exterior and interior doors. Authorized Mesa County employees can be granted access by the issuance of an access badge or card. Access card authorization is managed by the county's Human Resources (HR) department, which directs Mesa County Facilities Department staff to issue and program the cards. The Mesa County Facilities Department manages card reader access and retains logs of when authorized card holders accessed particular rooms. According to county employees, however, a person can "piggyback" behind an authorized card holder as the authorized card holder enters the room, so that the log would reflect only that the authorized card holder entered.

34. As of May 2021, the Clerk and Recorder's Office had a relatively straightforward hierarchy, according to interviews with multiple employees of the office. Serving below [REDACTED] was Deputy Clerk [REDACTED]. Under [REDACTED] [REDACTED] served as the director of elections. And under [REDACTED] [REDACTED] and [REDACTED] served as elections managers. This organizational hierarchy of the elections branch of the Mesa County Clerk and Recorder's Office, as of May 2021, is depicted below:⁷

⁷ There are numerous other employees in the elections branch of the Clerk's Office who are not relevant for purposes of this affidavit.



E. Preparations for the May 2021 Mesa County Trusted Build

35. According to public reporting, in the months following the 2020 national election, ██████ made multiple comments on her personal Twitter account (██████████) that have since been deleted. In response to a series of Tweets from a U.S senator denouncing efforts to challenge the national Electoral College certification, ██████ stated in January 2021: “Shame on you! As one that administers elections in my county, you apparently have no idea how it is possible to 1) tabulate more than once ballots favoring a candidate 2) change algorithm in a voting machine (see ██████ from Dominion’s Facebook ranks) UR Dirty or ignorant.”⁸ ██████ also stated that “[t]his was not an election. This was planned fraud on a grand scale. If you refuse to acknowledge that you WILL NOT be re-elected. We need others in your place that uphold the Constitution and preserve our Republic.”

⁸ ██████, Dominion’s security director, was forced into hiding after he became the victim of threats based on a conspiracy theory that he illegally switched votes on Dominion voting machines from one presidential candidate to another in the 2020 election.

36. Beginning in or around April 2021, according to e-mail traffic obtained voluntarily from Mesa County, the Colorado Secretary of State's Office commenced preparations for Trusted Build election software upgrades across Colorado, including in Mesa County.⁹ Mesa County's Trusted Build was scheduled to occur between May 25, 2021, and May 27, 2021.

37. On April 16, 2021, [REDACTED], the voting systems manager for the Colorado Secretary of State, contacted [REDACTED] at her Mesa County email address. [REDACTED] stated that he was "follow[ing] up on your request to have members of the public onsite during the trusted build of your voting equipment." [REDACTED] explained that "[o]nly required person[nel] from [Dominion], [the Secretary of State's Office], and the county will be permitted in the area of the trusted build." According to a subsequent interview of [REDACTED] conducted by 21st Judicial District Attorney's Office investigators, [REDACTED] had asked [REDACTED] to seek the Colorado Secretary of State's approval for community members to be present for the Trusted Build.

38. That month, according to an interview with one Clerk's Office employee, [REDACTED] used her Mesa County email address to send county elections staff a "save the date" calendar invite for an event on April 23, 2021. The purpose of the event was not specified, but the calendar invitation indicated that attendance was mandatory for [REDACTED].

⁹ Colorado law charges the Secretary of State with "supervis[ing] the conduct of . . . elections" as well as "inspect[ing] . . . and review[ing] the practices and procedures of county clerk and recorders." Colo. Rev. Stat. § 1-1-107. County Clerk and Recorders, in turn, must "follow the rules and orders promulgated by the secretary of state pursuant to [the state election code]." Colo. Rev. Stat. § 1-1-110(1).

F. Meeting with [REDACTED] at the Clerk and Recorder's Office in April 2021

39. On April 23, 2021, the day of the mandatory event and during business hours, [REDACTED] convened a meeting in her office. One meeting participant surreptitiously recorded partial audio from the meeting on a cell phone and subsequently provided that recording to investigators. Those in attendance from the Clerk and Recorder's Office were [REDACTED]. Non-employees present for the meeting included [REDACTED].

40. During the meeting on April 23, 2021 (based on the partial recording), [REDACTED] asserted that Mesa County's election management system was vulnerable to outside interference and was likely accessible remotely (by outside computers). [REDACTED] asked if [REDACTED] could open the voting machines. [REDACTED] responded that opening the machines was "against the law because you signed a contract." [REDACTED] responded: "Ok, all right, all right." [REDACTED], the local activist, raised the issue of the Mesa County Trusted Build set for late May: "On May 26-27, when they come, what's the plan?" One of the employees responded: "The plan, as far as I know, they're updating the software." [REDACTED] then asked [REDACTED]: "I'm gonna step out on a limb, you wanna come May 26?" [REDACTED] explained to [REDACTED] that "they're doing an audit here, they're gonna wipe the machines." [REDACTED] responded, "I don't think I'm your guy to do that audit, but I know the team and they'll do it for you and they'll come in with the best in the country." [REDACTED] then asked [REDACTED] to leave the room ("[REDACTED] might have to leave while we talk about this. . . . Why don't you leave while we talk about this?") and subsequently asked [REDACTED] to depart as well ("[REDACTED] you might need to walk out, too.").

41. According to interviews with two Clerk's Office employees, on the evening of April 23, 2021, the same day as the above-described meeting, Mesa County elections supervisors

(at [REDACTED] direction) attended a public presentation by [REDACTED] at the DoubleTree Hotel in Grand Junction, Colorado. According to the Facebook event description and [REDACTED] own Facebook posts, [REDACTED] served as an organizer for the event. One Clerk's Office employee later described the event as [REDACTED] presenting his theory of how election results could be manipulated.

G. [REDACTED] Linked to Network Access in Lake County, Ohio, on May 4, 2021

42. Approximately two weeks after the in-office meeting and the DoubleTree event described immediately above, there is evidence that [REDACTED] accessed the computer network for the government of Lake County, Ohio. As explained below, information from the Lake County network was subsequently copied and published online in connection with Lindell's August 2021 Cyber Symposium. It is currently believed that no voting machines or voting machine networks were accessed.

43. During the Cyber Symposium, links to download various data obtained from several counties around the country were released to the public via BitTorrent, a peer-to-peer filesharing network. The data dump included computer network packet capture files with the filenames, "LakeCounty_Main.pcapng," "LakeCounty_Main2.pcapng," "LakeCounty_Main3.pcapng," and "LakeCounty_Main4.pcapng." (Computers communicate on a data network by sending and receiving data packets. Specialized software applications are used to intercept and record the data packets as they are transmitted over a computer network. This capability is commonly referred to as a "packet capture" and the recorded data packets are commonly saved as a PCAP or PCAPNG file, *i.e.*, a "packet capture" file.)

44. On social media, individuals who had obtained copies of the "LakeCounty_Main" PCAP files analyzed them and began to report that the packet captures appeared to have been acquired from a computer network in Lake County, Ohio. This news prompted the Ohio Secretary

of State to investigate the matter. The Lake County Chief Information Officer “determined that a private laptop was plugged into the [Lake County] county network in [the county office of ██████████, president of the Lake County Board of Commissioners].”¹⁰

45. The four “LakeCounty_Main” PCAP files were also analyzed by FBI computer scientists and investigators. The date of capture was determined to have been May 4, 2021. Additional detail identified in the PCAP files indicated that the computer device that had recorded the packet capture data had a physical Ethernet adapter with a Media Access Control (MAC)¹¹ address of “██████████,” which was manufactured by Hewlett-Packard. The capture device hardware was a computer identified as an “AMD Ryzen 7 4800H with Radeon Graphics (with SSE4.2)”¹² running an operating system of “64-bit Windows 10 (1909), build 18363,” and with packet capture application “Dumpcap (Wireshark) 3.4.5 (v3.4.5-0-g7db1feb42ce9).”

46. ██████████ resides in Topanga, California, according to T-Mobile subscriber information and bank records in ██████████ name. Airline ticket records and records obtained by investigators for a known hotel only twenty minutes by car from Painesville, Ohio (the county seat for Lake County), indicated that ██████████ was present in Lake County, Ohio, on May 4, 2021—the day the “LakeCounty_Main” PCAP files were created. Records obtained by investigators also

¹⁰ See https://www.washingtonpost.com/politics/attempted-breach-ohio-election/2021/11/19/12417a4c-488c-11ec-b8d9-232f4afe4d9b_story.html.

¹¹ A MAC address is a hardware identification number that uniquely identifies each device on a network.

¹² SSE4.2 stands for Streaming SIMD Extensions, version 4.2. It is a series of instructions that can increase computer performance. As described below, the particular computer hardware and software (including version number) identified here is relevant because it appears that a computer with the same hardware, operating system, and packet capture application was used to obtain packet capture data from Mesa County systems—thus linking the two network intrusions.

revealed the following telephone communications between Lindell and [REDACTED] on or about May 4, 2021:

Date/Time	From	To	Communication
2021-05-04 17:29:11 UTC	Lindell Cellphone	[REDACTED]	Call forwarded to [REDACTED] ¹³
2021-05-04 17:29:56 UTC	Lindell Cellphone	[REDACTED]	Call forwarded to [REDACTED]
2021-05-04 17:42:53 UTC	[REDACTED]	Lindell Cellphone	Voice (1 min 24 sec)
2021-05-04 17:44:25 UTC	[REDACTED]	Lindell Cellphone	Voice (12 sec)

47. Investigators determined that the “LakeCounty_Main_2.pcapng” packet capture was recorded on 2021-05-04 from 16:51 UTC to 17:57 UTC. As documented in the call log for that day, Lindell and [REDACTED] were in communication with each other during the time of the packet capture’s acquisition.

H. Mike Lindell Wired \$100,000 to [REDACTED] on May 10, 2021

48. Approximately six days after the event in Lake County, Ohio, described above, Lindell paid [REDACTED] \$100,000.

49. Bank records obtained by investigators for a personal account associated with [REDACTED] revealed that on May 10, 2021, [REDACTED] received a wire transfer from Lindell Management LLC (a business entity associated with Mike Lindell) in the amount of \$100,000.00. Records

¹³ Analysis of communication records obtained from T-Mobile for [REDACTED] indicated that calls either to the [REDACTED] or telephone number [REDACTED] connected to the same mobile device linked to [REDACTED] which had an International Mobile Equipment Identity (IMEI) of [REDACTED]. Analysis of records obtained from Apple revealed that [REDACTED] had a phone application called “Burner” installed on his iPhone and had an active “Burner Subscription” plan at this time. The “Burner” app is advertised as “the market-leading second phone number app that allows you to have multiple numbers for multiple reasons.” See <https://apps.apple.com/us/app/burner-text-call-message/id505800761>.

obtained by investigators also revealed the following telephone communications between Lindell and [REDACTED] on or about May 10, 2021:

Date/Time	From	To	Communication
2021-05-10 03:57:17 UTC	Lindell Cellphone	[REDACTED]	Voice (23 min 40 sec)
2021-05-10 16:27:49 UTC	Lindell Cellphone	[REDACTED]	Voice (4 min 31 sec)
2021-05-10 19:48:09 UTC	Lindell Cellphone	[REDACTED]	Voice (31 sec)
2021-05-10 21:27:52 UTC	[REDACTED]	Lindell Cellphone	SMS text

I. Efforts to Obtain Access to Mesa County Trusted Build for [REDACTED], Posing as “[REDACTED]”

50. In this same general time period, efforts were underway in Mesa County, Colorado, to enable [REDACTED] to surreptitiously create forensic images of the Mesa County CVM both before and after the May 2022 Trusted Build described above in Section E.

51. On April 26, 2021, Colorado Secretary of State Voting Systems Manager [REDACTED] emailed [REDACTED] and other clerks throughout the state, explaining that an update to Dominion’s Democracy Suite voting system software had been certified for use in Colorado. [REDACTED] stated that Colorado would begin preparing for the voting system upgrades (that is, the Trusted Builds).

52. On April 30, 2021, [REDACTED] emailed a “Trusted Build Procedures” document to Clerks and Recorders across Colorado, including [REDACTED]. On the cover page for the document, [REDACTED] highlighted certain Trusted Build procedures, including: “Only authorized state staff, county election staff and Dominion staff may be present during the trusted build.” [REDACTED] explained that the “onsite installation of the Trusted Build is not the time for members of the public, representatives from the local parties, or county officials other than the Clerk & Recorder to observe or ask questions about the process or any of the disinformation being pushed about the election.” Secretary of State officials earlier had rejected efforts by Mesa County officials to

include members of the community in the Trusted Build and had clarified that only authorized personnel would be permitted in the Trusted Builds.

53. On May 13, 2021—notwithstanding the Secretary of State’s admonition limiting county representatives at the Trusted Build to “county election staff”—Deputy Clerk [REDACTED] called Mesa County HR Director [REDACTED] and left a voicemail requesting access permissions and a Mesa County e-mail account for an “IT person.” In the voicemail, [REDACTED] explained:

We have need to have an IT person come in while we’re doing some work on our election equipment and we would like for them to have their own badge so they have access to the election department doors as well as having a Mesa County email so that we can communicate with them. Is that possible for you to do? Do I have to put ‘em in as a temp employee? Do they have to go through our background check? What do we need to do? I mean, they will already go through the background check for elections, but do they have to go through one for HR? Can we just send them over to get a badge? Do you do the picture with a badge, is it just a straight badge? Just need to get some information for him.

54. On May 14, 2021, [REDACTED] emailed [REDACTED] using her Mesa County email address, stating, “Good morning, we would like to send someone to get their badge today if possible.” In a subsequent email that same day, [REDACTED] explained to [REDACTED] “I’m going to ask [REDACTED] to go get his badge for Elections access. Please take his photo and give him the same permissions as [Clerk and Recorder Elections [REDACTED]] [REDACTED].” Minutes later, [REDACTED] emailed her own staff in the HR Department: “FYI, in case I am not here. [REDACTED] is not a County employee he just needs a badge.”

55. On May 17, 2021, Deputy Clerk [REDACTED] approached Elections Manager [REDACTED] with a paper authorization form requesting a background check for [REDACTED].¹⁴ [REDACTED]

¹⁴ Under the Colorado Secretary of State’s Election Regulations, “all permanent and temporary county staff and all vendor staff who have access to the voting system or any voting or counting

explained that [REDACTED] was being hired as an “administrative assistant.” During a subsequent interview with 21st Judicial District Attorney’s Office investigators, [REDACTED] explained that she has conducted between 175 and 200 background checks of election judges and other officials who must pass a background check to volunteer or work with County Elections staff. [REDACTED] stated that [REDACTED] was the only individual [REDACTED] had never met while conducting an individual background check. In addition, [REDACTED] did not receive the paperwork that is typically included for a background check of a new employee. Nevertheless, [REDACTED] conducted the background check and [REDACTED] passed.

56. On May 18, 2021, [REDACTED] used her Mesa County email address to email Secretary of State’s Office Voting Systems Manager [REDACTED] to confirm that Mesa County would “adhere to the procedures outlined in your previous email during the trusted build installation”—presumably referring to [REDACTED] April 30, 2021, email. [REDACTED] stated that the “Mesa County staff that will be present” would be:

[REDACTED] – Elections Manager Back Office
 [REDACTED] – Administrative Assistant
 [REDACTED] – Mesa County Clerk & Recorder

[REDACTED] responded to [REDACTED] that [REDACTED] would list [REDACTED] as one member of the “authorized county staff.”

57. On May 19, 2021, [REDACTED] instructed [REDACTED] to go to Mesa County’s Human Resources department to obtain his access badge. On the afternoon after [REDACTED] obtained his county access badge, he was further directed by [REDACTED] to meet with herself and [REDACTED] to

equipment must pass a criminal background check.” 8 Colo. Code Regs. § 1505-1:11.1.3; *see also* 8 Colo. Code Regs. § 1505-1:20.5.3(a) (“Any person who has been convicted of an election offense or an offense with an element of fraud is prohibited from having access to the above areas.”). This involves sending a request to the Colorado Bureau of Investigation for a criminal history query.

discuss potential future work for [REDACTED] in the elections office. At the end of the meeting, [REDACTED] was required to return the access badge to [REDACTED] before he left the elections office. Later that evening and into the next morning, [REDACTED] exchanged SMS text messages.

Date/Time	From	To	Communication
2021-05-20 03:26:43 UTC	[REDACTED]	[REDACTED]	SMS text
2021-05-20 14:37:00 UTC	[REDACTED]	[REDACTED]	SMS text

58. On May 20, 2021, at 15:00:00 UTC (or 9:00 a.m. Mountain Time), records from Hotels.com indicate that [REDACTED] booked a room at a hotel in Grand Junction, Colorado, on her credit card for “[REDACTED].” The time of [REDACTED] booking was 23 minutes after her cellphone received an SMS text message from the [REDACTED].

59. According to subsequent interviews with county employees, including staff from the Mesa County HR Department, [REDACTED] was at no time employed by Mesa County. According to Mesa County Financing staff, [REDACTED] was never paid by the county.

60. As described below, access records show that a person using [REDACTED] badge accessed the Mesa County Elections Office on Sunday, May 23, 2021 (two days before the Trusted Build), and Tuesday, May 25, 2021 (the day of the Trusted Build). Subsequent investigation has revealed that [REDACTED] was likely not the individual using the access badge in his name, and that he was not present at the Mesa County Clerk and Recorder’s Office at any time from May 22, 2021, to May 27, 2021. For example, [REDACTED] stated in a February 2022 interview with investigators that he was not present in the Clerk and Recorder’s Office at any time from May 22, 2021, to May 27, 2021. Indeed, he stated that [REDACTED] and [REDACTED] took his access badge from him almost

immediately after it was issued, and he was not allowed to leave the Clerk and Recorder's Office with the badge in his possession.

61. Additionally, a combination of flight records, hotel records, and other information described below indicates that [REDACTED] traveled to Mesa County on May 22, 2021, from California. In this regard, hotel records for a known hotel in Grand Junction, Colorado (the county seat for Mesa County) indicate that [REDACTED] checked into that hotel on May 22, 2021, and checked out on May 26, 2021. Similarly, airline flight records indicate that [REDACTED] arrived in Grand Junction on May 22, 2021, and departed Grand Junction on May 26, 2021.

62. Further, according to an interview with [REDACTED] conducted in June 2022, she, along with [REDACTED], obtained access credentials for [REDACTED] for the express purpose of giving them to [REDACTED] so that he could access the CVM and the Trusted Build.¹⁵ [REDACTED] also asserted that [REDACTED] told her that [REDACTED] gave permission for [REDACTED] to use [REDACTED] Mesa County access credentials to gain access to the CVM and the Trusted Build. In his February 2022 interview with investigators, however, [REDACTED] denied having any awareness at the time he was provided his access credentials that they would be used by someone else.

J. [REDACTED] Orders Cameras Disabled in the Clerk and Recorder's Office

63. According to a service ticket obtained from staff in the Mesa County IT Department, on May 17, 2021, [REDACTED] requested that the IT Department shut off the security

¹⁵ [REDACTED] sat for this interview with Mesa County investigators and attorneys as well as attorneys for the U.S. Department of Justice and the Colorado Attorney General's Office. [REDACTED]

camera system for the Clerk and Recorder's Office. IT staff member [REDACTED] shut off the camera system as directed.

64. In a subsequent interview with investigators, [REDACTED] stated that he was unaware of the purpose of [REDACTED] request. According to [REDACTED] no financial benefit accrues to the county by disabling the video recording system. Data storage costs, for example, are not impacted by disabling the camera. [REDACTED] also stated that he was unaware of any prior request in the last several years to shut off the camera system. Instead, it was more common for the IT Department to receive requests about whether the camera system was in working order prior to and during election periods.¹⁶

65. According to [REDACTED] subsequent statements to law enforcement, she contacted IT staff at or about the beginning of August 2021 to ensure that the camera system was in working order, to comply with state law. [REDACTED] was surprised to learn that the cameras had been off since approximately May 2021. [REDACTED] then requested that the cameras be re-enabled.

66. During a conversation between [REDACTED] and Deputy Clerk [REDACTED] regarding the disabling of the cameras, [REDACTED] informed [REDACTED] that the reason the cameras were turned off was to save the county money. [REDACTED] believed, however, that the county would reap no savings from disabling the cameras and that [REDACTED] explanation was not truthful. Additionally, in an interview with a Mesa County District Attorney's Office investigator on August 10, 2021, [REDACTED] stated that [REDACTED] directed [REDACTED] to shut off the cameras.

¹⁶ Under the Secretary of State regulations, "the county must make video security surveillance recordings . . . beginning at least 60 days before election day and continuing through at least 30 days after election day." 8 Colo. Code Regs. § 1505-1:20.9.2. According to both [REDACTED] and the Secretary of State's Office, however, Mesa County's general practice has been to regularly keep its cameras running even outside of the statutory recording window.

K. The CVM is Imaged Prior to the Trusted Build

67. As explained further below, and as [REDACTED] has admitted in recent civil litigation, [REDACTED] asked an individual she has characterized as a “consultant” to “image”¹⁷ the hard drive of the county’s electronic vote-tabulating equipment before and after the Trusted Build. These images were later posted to the Internet. As set forth in this affidavit, investigators believe that this “consultant” was [REDACTED]

68. On Sunday, May 23, 2021, two days before the Trusted Build in Mesa County, key card access records reflect that [REDACTED] [REDACTED] (likely [REDACTED] and [REDACTED] were present in the building at different times throughout the day. Logs reflect that (1) [REDACTED] entered different rooms, including the Tabulation Room, between 11:49 a.m. and 8:21 p.m.; (2) [REDACTED] entered various rooms between 3:53 p.m. and 6:50 p.m.; and (3) [REDACTED] entered different rooms, including the Tabulation Room, between 10:53 a.m. and 3:03 p.m. [REDACTED] and [REDACTED] therefore appear to have been alone in the Elections Office for multiple hours that Sunday evening, approximately 36 hours before the Trusted Build.

69. In an August 2021 televised interview with Lindell, [REDACTED] admitted that she was “concerned [that] vital statistics and information was being deleted from the system or could be deleted from the system and I decided to preserve that.” She explained that she “was suspicious that something was happening to that information” and that she “decided to make an image before” the Trusted Build.

70. In recent civil litigation involving the Colorado Secretary of State’s Office—which resulted in a decision that [REDACTED] may not continue to perform the duties of chief designated election

¹⁷ The term “image,” in the context of computer devices, is a technical term that is essentially synonymous with “copy.”

official for Mesa County—[REDACTED] admitted that she “authorized a consultant to take an image of the electronic vote-tabulating equipment hard drive prior to the trusted build process scheduled for May 25, 2021.”

L. The May 25 Trusted Build

71. On Tuesday, May 25, 2021, the Trusted Build upgrade was performed on the CVM at the Mesa County Elections Office. According to multiple interviews conducted with participants, [REDACTED], and another individual introduced as [REDACTED] (but who was likely in fact [REDACTED]) were present along with three Dominion staff and a Colorado Secretary of State Senior Voting Systems Specialist.

72. According to an August 2021 interview of the Voting Systems Specialist, [REDACTED] explained during the Trusted Build that [REDACTED] was currently working at the county’s Department of Motor Vehicles but was transferring to the Elections Office.¹⁸ Badging access records for the badge in [REDACTED] name reflect that the user of that badge was present in multiple Elections Office rooms including the Tabulation Room throughout May 25, 2021. Aside from the logs reflecting the [REDACTED] badge’s access on May 23, 2021 (described above) and the logs reflecting [REDACTED] access on May 25, 2021, there is no indication from the badging access records that [REDACTED] was ever present in the Mesa County Clerk and Recorder’s Office between May 23, 2021, and May 27, 2021.

¹⁸ As noted, Clerk’s Office officials had already characterized [REDACTED] as an “administrative assistant,” a member of the “Mesa County staff,” and an “IT Person,” despite county records reflecting that [REDACTED] was never employed by or paid by the county. Additionally, on October 28, 2021, the Mesa County Commissioners received an email signed by “[REDACTED]” from the email address [REDACTED]. In that email, the author identified “[REDACTED]” as her husband. The author further stated that “[REDACTED] has worked as a software engineer for the same company for 29 years and NEVER for the DMV.”

M. The CVM is Imaged Following the Trusted Build

73. [REDACTED] has admitted in the above-described civil litigation that on or about May 26, 2021 (the day following the Trusted Build), she authorized the same “consultant”—likely [REDACTED]—to image the CVM for a second time. In the previously mentioned August 2021 televised interview with Lindell, [REDACTED] also admitted that she made a copy of the CVM after the Trusted Build upgrade. [REDACTED] explained that she copied the system before and after the Trusted Build because she was suspicious of the upgrade. [REDACTED] also admitted in the civil litigation that, “[s]hortly after the trusted build process,” she authorized “the same consultant to take another forensic image of the electronic vote-tabulating equipment hard drive.”

74. On Wednesday, May 26, 2021, badging records indicate that only two individuals were present at the Elections Office after 23:00 UTC (or 5:00 p.m. Mountain Time): [REDACTED] and [REDACTED]. For example, [REDACTED] entered the Tabulation Room at 5:53 p.m. Mountain Time, at a time when badging access records show that only she and [REDACTED] were present at the Elections Office. Similarly, [REDACTED] was in the Tabulation Room from 5:39 p.m. to 6:28 p.m. Mountain Time, and from 6:30 p.m. to 6:59 p.m. Mountain Time. The [REDACTED] access badge does not appear to have been used on May 26, 2021, at the Mesa County Clerk and Recorder’s Office.

75. On or about Thursday, May 27, 2021, a Mesa County employee named [REDACTED] mailed a package from a Grand Junction, Colorado, United States Postal Service office to [REDACTED] at a California residence. [REDACTED] wrote on the United States Postal Service form that the sender was “Mesa Co. Clerk & Recorder [REDACTED].” The timing of this mailing is consistent with [REDACTED] departing Grand Junction on May 26, 2021, before the completion of the second forensic image, with the understanding that [REDACTED] would arrange for the image to be sent to [REDACTED] once it was finished.

N. **Similarities Between the Lake County Network Breach and the Mesa County Incident Indicate That [REDACTED] Participated in Both Events**

76. Forensic evidence suggests that [REDACTED] was involved in both the Lake County network breach and the Mesa County breaches described above.

77. First, the same laptop was likely present in Lake County during its network breach and in Mesa County during the May 2021 Trusted Build. Investigators determined that the same laptop was likely present at these two incidents based on an analysis of packet capture (or “PCAP”) files originating from these two locations that were subsequently posted on the Internet and discussed at the Lindell symposium in August 2021.

78. In this regard, the BitTorrent data dump of files from the Cyber Symposium in August 2021 contained network packet capture files from Mesa County, in addition to the packet captures from Lake County, Ohio, discussed previously. To be clear, the Mesa County PCAP files are distinct from the Mesa County CVM images discussed elsewhere in this affidavit. The “Mesa” PCAP files were also analyzed by FBI computer scientists and investigators and their date of capture was identified to be May 23, 2021 (at a time when [REDACTED] was also in Mesa County). Details within these PCAP files indicated that the computer device that had recorded the packet captures had a Wi-Fi Ethernet adapter with a MAC address of “[REDACTED]” manufactured by Intel Corporation.

79. Overall, the analysis revealed a high likelihood that the same computer was used to acquire both the Lake County and Mesa County packet captures. The computer used to acquire the data in both counties ran the exact same hardware (“AMD Ryzen 7 4800H with Radeon Graphics (with SSE4.2)”); the exact same operating system, with the same updates (“64-bit Windows 10 (1909), build 18363”); and the exact same packet capture application (“Dumpcap (Wireshark) 3.4.5 (v3.4.5-0-g7db1feb42ce9)”). The presence of the Wireshark application itself is particularly

notable because it is not commonly found on most Microsoft Windows computer systems (the application is not installed by default). Rather, Wireshark is a specialized tool installed and used primarily by computer network and computer security professionals to examine and troubleshoot networks.

80. While the MAC addresses associated with the acquisition computer used in the two counties did differ, that is explained by the difference in how the packet captures were acquired. A MAC address is unique per Ethernet adapter and computers commonly have more than one network adapter, *e.g.*, a wired and a wireless adapter. In Lake County, the captures were made via the acquisition computer's wired or physical Ethernet adapter (*i.e.*, the acquisition computer was plugged into the network via a cable), whereas in Mesa County the captures were made via the acquisition computer's wireless or "Wi-Fi" network adapter.

81. Second, and as described earlier, flight, hotel, and financial records also placed ██████████ in both counties on the exact dates when both captures were recorded. Investigators have accordingly assessed that ██████████ participated in both the Lake County and Mesa County breaches using the same laptop computer.

82. Telephone records obtained by investigators revealed that Lindell and ██████████ were also apparently in telephone communication while ██████████ was in Mesa County on or about May 24, 2021 (on the evening before the May 25, 2021, Trusted Build):

Date/Time	From	To	Communication
2021-05-24 15:21:18 UTC	Lindell Cellphone	██████████	Recorded in toll log as "Abnormal Completion." ¹⁹
2021-05-24 19:17:05 UTC	██████████	Lindell Cellphone	Voice (8 min 50 sec)

¹⁹ Investigators cannot assess with certainty whether this call was completed.

2021-05-24 20:14:27 UTC	Lindell Cellphone	██████████	Voice (1 min 30 sec)
2021-05-24 21:32:10 UTC	Lindell Cellphone	██████████	Voice (5 sec)
2021-05-24 22:46:37 UTC	██████████	Lindell Cellphone	Voice (3 sec)

83. Based on the timing of ██████████ travel to Mesa County compared with the generation of badge access credentials in ██████████ name, coupled with the other circumstances identified in this affidavit, there is probable cause to believe that ██████████ along with other individuals including ██████████, and Lindell, committed identity theft and conspired to commit that offense, in violation of 18 U.S.C. §§ 1028(a)(7) and 371, by impersonating ██████████ ██████████ with the intent of committing the Colorado state law felony of attempting to influence a public servant, in violation of Colorado Rev. Stat. § 18-8-306. In this regard, by unlawfully using ██████████'s identifying information to infiltrate the Trusted Build, ██████████ deceived Colorado Secretary of State personnel into thinking that he was a legitimate Mesa County employee with a right to be present for the Trusted Build on behalf of the Mesa County government. There is also probable cause to believe that this impersonation of ██████████ was undertaken to further these same individuals' violation of 18 U.S.C. § 1030(a)(5).

O. ██████████ Statements to the Ohio SOS About Teaming up with Mike Lindell and Computer Forensic Experts Who Will Work "Under the Radar"

84. On or about May 27, 2021, ██████████ met with staff from the Ohio Secretary of State's Office to discuss ██████████ purported discovery of widespread election fraud in Ohio. The meeting lasted nearly two hours and was recorded by staff from the Ohio Secretary of State's Office. A copy of the recording was provided to the FBI. In the meeting, ██████████ said that he was working with the "Lindell team and the President" and that "[the Lindell team], because of ██████████ work around the country, [the Lindell team] has plants everywhere. [They] go into buildings where your machines are on and capture your IP addresses."

85. On the recording, [REDACTED] described his prior involvement with the team of forensic experts as follows:

In the places where [REDACTED] and local election officials] work together, I brought in teams. Because I have access to some of the best forensic teams in the country. And they will come in and they will look at everything for you. And they will find any problems that you have. And in that case they are not just coming in trying to expose you and make you look bad. They're coming in to help you try and find your problems and fix them. We have counties in multiple states who are cooperating. Under the radar. On that level.

86. On the recording, [REDACTED] also described how quickly he could bring in a team of forensic experts:

I can make a phone call right now and there will be a team of forensic experts here that will do forensic images of all of the machines and all of the systems in a few days.

P. Mike Lindell Wired \$100,000 to [REDACTED] on July 8, 2021.

87. Bank records obtained by investigators for an account associated with [REDACTED] revealed that on July 8, 2021, [REDACTED] received a wire transfer from Lindell Management LLC in the amount of \$100,000.00. Records obtained by investigators also revealed the following telephone communications between Lindell and [REDACTED] on or about July 8, 2021:

Date/Time	From	To	Communication
2021-07-08 03:17:38 UTC	Lindell Cellphone	[REDACTED]	Voice (33 min 4 sec)
2021-07-08 16:43:32 UTC	Lindell Cellphone	[REDACTED]	Voice (2 min 36 sec)

Q. Mesa County Election Management System Passwords and Data Leak on the Internet

88. On or about August 3, 2021, via the end-to-end encrypted messaging service Telegram, [REDACTED], who is also known by his online moniker/username as "[REDACTED]," posted photographs and a video purportedly taken by a Dominion "whistleblower." [REDACTED] is a

prominent espouser of conspiracy theories related to the 2020 presidential election. The photographs and video quickly began circulating on the Internet and were shared on social media websites.

89. The photographs contain a list of BIOS passwords purportedly for Dominion elections computers and instructions on system login and procedures, including how to access the internal system BIOS. The video appears to have been taken from a cell phone camera and depicts the screen activity of a computer monitor. The screen displays a “Dominion Voting” logo and shows a date of May 25, 2021—the day of the Trusted Build upgrade for Mesa County. The voices on the video discuss, among other things, who holds the passwords to the system (“The state won’t let us have our own passwords?”) and the system’s Internet connectivity.²⁰ The voices sound as if they have been altered or dampened to conceal the identity of the speakers. In recent civil litigation, ██████ admitted that she “took a video and still photographs of the trusted build process on May 25, 2021.”

90. On or about August 3, 2021, Secretary of State representatives reviewed the released photographs and video. According to the Secretary’s representatives, the photographs captured the specific BIOS passwords or codes it had solely maintained for the Dominion elections computers at Mesa County and which were used during the May 25, 2021, Trusted Build. The photographs also apparently contained software and system access instructions particular to Dominion elections computers. Additionally, according to the Secretary’s representatives, the CVM equipment visible in the released video is the same type of equipment used by Mesa County.

²⁰ At present, investigators do not have reason to believe that the CVM was connected to the Internet at any relevant time.

91. Having recognized that the BIOS passwords and video released on the Internet were likely taken from the May 25, 2021, Trusted Build process in Mesa County, the Colorado Secretary of State initiated an inspection of the CVM equipment in Mesa County on or about August 10, 2021. During the inspection, a Colorado Secretary of State Voting Systems Specialist found that two BIOS settings had been changed from the baseline configuration set at the end of the Trusted Build. The changed settings (1) disabled Secure Boot, a feature that helps make sure that a computer boots (*i.e.*, starts) using only trusted software, and (2) enabled the option to boot from the Optical Drive, which would allow the CVM to boot from optical media such as a CD or DVD.

92. These modifications could not have been made without the BIOS passwords. According to a Colorado Secretary of State Voting Systems Specialist, these passwords are sometimes referenced in Dominion procedures as the BIOS “setup” passwords. It was the BIOS “setup” passwords that were leaked online on August 3, 2021, as described above. These same procedures also reference a BIOS “Admin” password, but this password is typically configured to be empty and is not sufficient to change the two settings described above. According to this same Voting Systems Specialist, the Colorado Secretary of State took custody of the BIOS “setup” passwords in or about 2019; Colorado counties no longer had access to these passwords after 2019.²¹

²¹ I, along with other members of the investigative team, have reviewed a Dominion manual describing the Trusted Build Process for Colorado in 2021. According to the Colorado Secretary of State Voting Systems Specialist, this document contains certain errors. For instance, at one point, the manual erroneously lists the “county” as being responsible for setting a BIOS “setup” password. Members of the investigative team have confirmed with the Secretary of State voting system specialist that this is no longer accurate, and that the Secretary of State retains sole custody of BIOS “setup” passwords.

93. Separately, two data sets were posted on the Internet that purport to be images of the Mesa County election management system server (that is, the CVM) before and after the Trusted Build. One of the images contains Dominion's Democracy Suite Version 5.11, the software version used by Mesa County before the Trusted Build, and appears to have been created on Sunday, May 23, 2021 (the day that [REDACTED] [REDACTED] (likely [REDACTED] and [REDACTED] were present late in the evening at the Elections Office). The second image contains Dominion's Democracy Suite Version 5.13, the software version used by Mesa County after the Trusted Build, and appears to have been created on Wednesday, May 26, 2021 (another day that [REDACTED] and [REDACTED] were present in the evening at the Elections Office). [REDACTED] stated during an August 2021 interview with Lindell that she "did not post, did not authorize anyone to post any election data or software or passwords online." According to Dominion officials, the CVM images contain proprietary Dominion data and software, which was released in violation of Mesa County's contract with Dominion.

R. August 2021 Events Following the Data Leak

94. On August 9, 2021, at about 16:15 UTC, the Colorado Secretary of State sent Election Order 2021-01 to [REDACTED]. The order was sent in response to the Colorado Secretary of State's recognition that the BIOS passwords leaked by [REDACTED] on August 3, 2021, were the Colorado Secretary of State Office's BIOS passwords for Mesa County. Among other requests in the order, the Colorado Secretary of State Office directed [REDACTED] to identify "all representatives of the Mesa County Clerk and Recorder's office who participated in" the May 2021 Trusted Build. While [REDACTED] did not comply with the election order, the circumstances surrounding the order spurred a significant number of communications involving [REDACTED]

█████ Lindell, █████ and others. The table below is a partial list of these communications along with some of the notable events:

Date/Time	From	To	Communication
2021-08-09 00:01 UTC	Lindell Cellphone	█████	Voice (8 min 29 sec)
2021-08-09 00:10 UTC	Lindell Cellphone	█████	Voice (42 sec)
2021-08-09 00:12 UTC	Lindell Cellphone	█████	Voice (7 min 54 sec)
2021-08-09 00:24 UTC	Lindell Cellphone	█████	Voice (5 min 43 sec)
2021-08-09 00:33 UTC	Lindell Cellphone	█████	Voice (4 min 54 sec)
2021-08-09 00:42 UTC	Lindell Cellphone	█████	Voice (2 min 49 sec)
2021-08-09 04:18 UTC	█████	Lindell Cellphone	Voice (35 min 23 sec)
2021-08-09 15:07 UTC	Lindell Cellphone	█████	Voice (7 min 3 sec)
2021-08-09 16:00 UTC	█████	Lindell Cellphone	SMS text
2021-08-09 16:01 UTC	█████	Lindell Cellphone	Voice Mail (26 sec)
2021-08-09 16:15 UTC	Colorado SOS Election Order 2021-01 delivered to █████ via Email		
2021-08-09 17:26 UTC	█████ ²²	█████ ²³	SMS text

²² FBI personnel used a variety of open sources, law enforcement databases, and records returned by Verizon in October 2021 in response to an 18 U.S.C. § 2703(d) court order and established that an Apple iPhone SE 256GB White cellular device, IMEI █████, with telephone number █████ was associated with █████. This phone was not found during the search of █████ residence at █████, pursuant to federal search warrant issued in the District of Colorado (█████) and executed on November 16, 2021.

²³ FBI personnel used a variety of open sources, law enforcement databases, and records returned by Verizon in October 2021 in response to an 18 U.S.C. § 2703(d) court order and established that a Samsung Galaxy S10e cellular device with telephone number █████ was associated with █████. This phone was collected from █████ on November 16, 2021, pursuant to federal search warrant issued in the District of Colorado (█████), which was executed at her residence at █████. The phone is one of about 25 digital devices collected that day pursuant to four federal search warrants executed across four residences. The collected devices are currently undergoing an attorney-client privilege review.

2021-08-09 17:28 UTC	[REDACTED]	[REDACTED]	SMS text
2021-08-09 17:59 UTC	Lindell Cellphone	[REDACTED]	Voice (2 sec)
2021-08-09 18:03 UTC	Lindell Cellphone	[REDACTED]	Voice (2 sec)
2021-08-09 21:46 UTC	[REDACTED]	Lindell Cellphone	SMS text
2021-08-09 21:47 UTC	[REDACTED]	Lindell Cellphone	SMS text
2021-08-09 21:54 UTC	[REDACTED]	[REDACTED]	Voice (56 sec)
2021-08-09 21:56 UTC	[REDACTED]	[REDACTED]	Voice (37 sec)
2021-08-09 21:57 UTC	Lindell Cellphone	[REDACTED]	SMS text
2021-08-09 22:06 UTC	[REDACTED]	Lindell Cellphone	SMS text
2021-08-10 00:24 UTC	[REDACTED]	[REDACTED]	SMS text
2021-08-10 00:31 UTC	[REDACTED]	Lindell Cellphone	Voice (33 sec)
2021-08-10 00:43UTC	[REDACTED]	[REDACTED]	SMS text
2021-08-10 01:25 UTC	[REDACTED]	Lindell Cellphone	Voice Mail (27 sec)
2021-08-10 01:52 UTC	Lindell Cellphone	[REDACTED]	Voice (1 min 22 sec)
2021-08-10 01:59 UTC	Lindell Cellphone	[REDACTED]	Voice (12 min 53 sec)
2021-08-10 02:19 UTC	Lindell Cellphone	[REDACTED]	Voice (2 sec)
2021-08-10 02:20 UTC	Lindell Cellphone	[REDACTED]	Voice (2 min 27 sec)
2021-08-10 02:58 UTC	Lindell Cellphone	[REDACTED]	Voice (48 sec)
2021-08-10 02:59 UTC	Lindell Cellphone	[REDACTED]	Voice (1 min 9 sec)
2021-08-10 03:11 UTC	Lindell Cellphone	[REDACTED]	Voice (2 min 6 sec)
2021-08-10 04:00 UTC	Lindell Cellphone	[REDACTED]	Voice (20 sec)
2021-08-10 04:03 UTC	Lindell Cellphone	[REDACTED]	Voice (3 min 50 sec)
2021-08-10 13:31 UTC	[REDACTED]	Lindell Cellphone	SMS text
2021-08-10 14:16 UTC	Lindell Cellphone	[REDACTED]	SMS text
2021-08-10 14:16 UTC	[REDACTED]	Lindell Cellphone	SMS text
2021-08-10 14:17 UTC	[REDACTED]	Lindell Cellphone	SMS text

2021-08-10 15:40 UTC	[REDACTED]	Lindell Cellphone	SMS text
2021-08-10 16:09 UTC	[REDACTED]	Lindell Cellphone	SMS text
2021-08-10 16:09 UTC	[REDACTED]	Lindell Cellphone	SMS text
2021-08-10 16:56 UTC	Lindell Cellphone	[REDACTED]	SMS text
2021-08-10 17:03 UTC	[REDACTED]	Lindell Cellphone	SMS text
2021-08-10 17:09 UTC	[REDACTED]	Lindell Cellphone	SMS text
2021-08-10 17:13 UTC	[REDACTED]	Lindell Cellphone	SMS text
2021-08-10 17:13 UTC	Lindell Cellphone	[REDACTED]	SMS text
2021-08-10 17:19 UTC	[REDACTED]	Lindell Cellphone	SMS text
2021-08-10 18:45 UTC	Mesa County DA Investigator [REDACTED] [REDACTED]	[REDACTED]	Telephonic Interview: Investigator [REDACTED] asked [REDACTED] "Real quick do you know anything about anyone who was taking pictures or filming in there?" [REDACTED] replied, "You know what I will have to call you back, I am checking into this, because this is really upsetting, let me check into it and then I will call you back, I am boarding right now."
2021-08-10 19:17 UTC	Private jet "[REDACTED]", publicly reported on social media by multiple sources to belong to Mike Lindell, departed Grand Junction, CO (Source: FlightAware.com)		
2021-08-10 20:38 UTC	Private jet "[REDACTED]" landed in Sioux Falls, SD (Source: FlightAware.com)		
2021-08-11 00:29 UTC	Mike Lindell introduced [REDACTED] and [REDACTED] who is associated with [REDACTED] on stage at the Cyber Symposium. [REDACTED] asserted that [REDACTED] was standing up for what people were asking her to do (to protect their vote) and that [REDACTED] had come under duress by an "overreaching" and "overbearing" Secretary of State who was "lawless" and had "[weaponized] her office against [REDACTED]"		

	Lindell also stated: “I want to say something too. Remember I said when I came out here, we have a [technical] red team here. So, we are going to come back on Thursday . . . maybe we will find out why they raided [redacted] office. Stay tuned for Thursday.”		
2021-08-11 03:42 UTC	Lindell Cellphone		Voice (44 min 54 sec)
2021-08-11 10:41 UTC	First known public dissemination of Internet links to download the disk images of Mesa County’s election management server hard drive.		
2021-08-11 15:34 UTC	At Lindell’s Cyber Symposium, [redacted] and another individual are the first to announce the existence of “publicly available” files of Mesa County disk images.		
2021-08-12 02:13 UTC	Lindell Cellphone		Voice (22 min 45 sec)
2021-08-12 07:10 UTC	Lindell Cellphone		Voice (7 min)
2021-08-12 07:25 UTC	Lindell Cellphone		Voice (75 min 18 sec)

95. On or about August 10, 2021, as indicated in the table above, [redacted] and others flew from Grand Junction, Colorado, to Sioux Falls, South Dakota, to attend Lindell’s Cyber Symposium. Based on various Facebook posts from individuals associated with [redacted] [redacted] was accompanied on the plane by, among others, [redacted] (the local political activist who was present during the April 23, 2021, meeting with [redacted] in [redacted] office).

96. On the evening of August 10, 2021, [redacted] [redacted] and [redacted] appeared on stage with Lindell at the event. The group announced, in substance, that the Colorado Secretary of State had conducted an investigation on that date (August 10) at Mesa County’s elections offices. That investigation was related to (a) how passwords in the possession of the Colorado Secretary of State’s staff were surreptitiously recorded during a scheduled software update of election equipment in Mesa County on May 25-26, 2021, and (b) [redacted] refusal to obey the election order sent to Mesa County on August 9, 2021. [redacted] asserted that the Colorado Secretary of State was responsible for the loss of her passwords and that the Secretary of State’s

investigation in Mesa County was illegitimate and politically motivated. [REDACTED] speaking at Lindell's conference about the password leak, stated:

So I've been accused of passing down or allowing someone to expose our passwords in our elections office. And these just happen to be passwords that only the Secretary of State has. As a matter of fact, when they were in doing this trusted build in our office, they told me that I'm not allowed to have those passwords. That only they are. And so I question that because, we have passwords to get into our system. Why do they have passwords I can't have to get in the backdoor of our system. Why is that? I don't know. That's a question that we need answers to and we're gonna find it.

97. As indicated in the table above, a state investigator interviewed [REDACTED] by phone on August 10, 2021. [REDACTED] questioned whether the "whistleblower" video leak described above had in fact revealed passwords to Mesa County election infrastructure by asking, "Has that been proven?" She stated that it was "preposterous" to believe someone could have made a video during the May 25, 2021, Trusted Build, but then asked, "Is it illegal to take a video of [the Trusted Build]?" [REDACTED] then complained that the Secretary of State was politically motivated to remove [REDACTED] from office. She stated that the Secretary of State may be trying to "frame" her. When the investigator directly asked [REDACTED] if she was aware who might have been filming in the room, she said, "I'll have to call you back. . . this is really upsetting to me." Although the investigator sent his phone number to [REDACTED] she never contacted him.

98. As referenced by [REDACTED] at the symposium, on or about August 10, 2021, the Colorado Secretary of State initiated an inspection of Mesa County's election management system and the 21st Judicial District Attorney's Office in Colorado (*i.e.*, the District Attorney's Office covering Mesa County) executed a search warrant at the Mesa County Clerk and Recorder's office. The following day, August 11, 2021, the 21st Judicial District Attorney's

Office in Colorado executed a warrant at [REDACTED] residence and seized multiple electronic devices. These warrants are described in greater detail below.

99. The Colorado Secretary of State's Office ultimately de-certified the Mesa County election management server—prohibiting it from being used in future elections—because the office could not “establish confidence in the integrity or security” of the server.

100. Separately, the earliest record investigators have discovered of the “publicly available” files referenced during the Cyber Symposium—that purportedly contain copies of the pre- and post-Trusted Build Mesa County election management system server—is from on or about August 11, 2021, at 10:41 UTC.

101. The FBI obtained copies and analyzed the disk images released on the Internet and determined that they were captured on May 23, 2021, and May 26, 2021, respectively. Additionally, preliminary forensic analysis of the election management system server by the FBI indicated that the May 26, 2021, disk image may not have been *completed* until the morning of May 27, 2021, even if the imaging process began on May 26, 2021. Further analysis of the images on the Internet determined that the disk images had embedded information that included an “Examiner” data field, whose value would have been entered by the person acquiring the disk images. The value entered for the “Examiner” field for the two disk images from Mesa County was [REDACTED] which are the initials for [REDACTED].

102. On September 29, 2021, the FBI obtained a federal search warrant in the District of Colorado (Case No. 21-SW-00994-GPG) and seized control of the election management system's server and the other election computer systems maintained in Mesa County, Colorado, in May 2021. In a subsequent forensic examination of the election management system's server, investigators confirmed the reported findings from their preliminary forensic analysis of the disk

images that were released on the Internet. In addition, investigators identified the election management server to be a Dell Power Edge server, Model T630, which ran the operating system version, “Windows Server 2016 Standard (1607).” Investigators discovered forensic artifacts on the system indicating that on May 26, 2021, at approximately 23:34:55 UTC (or 5:34 p.m. Mountain Time), an external hard drive was attached to the system via USB port. Key card access records reflect that [REDACTED] was frequently entering and exiting the tabulation room during this time period.

103. Digital artifacts revealed that the computer operator at that time then launched the “FTK IMAGER.exe” application from the attached external hard drive. (The FTK Imager application is a digital forensic tool that can be used to acquire a forensic disk image of a running computer system.)

104. Investigators also discovered that a second external hard drive was attached via USB port to a second election computer system that was in Mesa County, Colorado, in May 2021. Investigators identified the second computer system to be a Dell Precision computer, Model T3420, which ran the operating system version, “Windows 10 Pro (1909).” Investigators discovered forensic artifacts on the system that the external hard drive was attached to the system on May 26, 2021, at approximately 23:34:45 UTC (or 5:34 p.m. Mountain Time). Digital artifacts revealed that the computer operator at the time then launched the “FTK IMAGER.exe” application from the attached external hard drive.

105. On August 11, 2021, at Lindell’s Cyber Symposium, [REDACTED] (appearing onstage as a session facilitator), [REDACTED] (appearing remotely via video as a computer expert), and another individual appearing onstage as a computer expert led a review of what was described as “publicly available” forensic image files of the hard drive from the Dominion election

management server in Mesa County, Colorado, from before and after Dominion's election computer upgrades in May 2021. When [REDACTED] introduced himself, he stated:

Recently a pair of publicly available files were brought to my attention. The files are allegedly forensic images of the Mesa County Colorado, Dominion election management system. I have not seen these files yet.

106. Furthermore, another individual at the event, described as a leader of Lindell's technical team, announced:

This information [the Mesa County forensic disk images] as well as [forensic disk images from a Michigan county's election system] will be available. Again, this was a publicly available file that, uh, [was] found yesterday afternoon, last night. And we will be able to point you to where that file was. Several of you asked, well, can we see this, can we look at it? Can we do the, you know, before and after comparison? [Can we] write a program, write a script, to do the forensic comparison? So, that's the intent.

107. Approximately three hours into the data review, [REDACTED] abruptly interrupted the session and made the following announcement:

We have a problem. . . . I just learned that [REDACTED] may have taken without authorization the actual hard drives from the Mesa Colorado County Clerk and he needs to produce those hard drives immediately and return them to the Clerk and we should stop this data review until he produces the hard drives.

108. There was confusion after [REDACTED] announcement at the event, but the data review continued. After some time had passed, [REDACTED] followed up with this revised statement:

So, the information that [REDACTED] [identified by [REDACTED] to be [REDACTED] lawyer] received was from [REDACTED] and now she has informed [REDACTED] that [REDACTED] did have permission to take the hard drive but did not have permission to upload it. [REDACTED] indicated to [REDACTED] that she was an affiliate of [REDACTED]. And now [REDACTED] is not sure whether that is in truth.

S. Mike Lindell Wired \$100,000 to [REDACTED] on August 17, 2021

109. Bank records obtained by investigators for a personal account associated with [REDACTED] revealed that on August 17, 2021, [REDACTED] received a wire transfer from Lindell Management LLC in the amount of \$100,000.00. Records obtained by investigators revealed the following telephone communications between Lindell and [REDACTED] on or about August 17, 2021:

Date/Time	From	To	Communication
2021-08-16 22:03:58 UTC	[REDACTED]	Lindell Cellphone	SMS text
*2021-08-17 02:55:02 UTC	Lindell Cellphone 2 ²⁴	[REDACTED]	Call forwarded to [REDACTED]
2021-08-17 04:24:33 UTC	[REDACTED]	Lindell Cellphone	Voice (1 sec)
2021-08-17 04:24:43 UTC	[REDACTED]	Lindell Cellphone	Voice Mail (9 sec)
2021-08-17 04:25:05 UTC	[REDACTED]	Lindell Cellphone	Voice Mail (2 sec)
*2021-08-17 04:25:22 UTC	Lindell Cellphone 2	[REDACTED]	Call forwarded to [REDACTED]
*2021-08-17 04:25:29 UTC	[REDACTED]	Lindell Cellphone 2	Voice (73 min 41 sec)
*2021-08-17 05:41:25 UTC	Lindell Cellphone 2	[REDACTED]	Voice (65 min 26 sec)
*2021-08-17 14:59:07 UTC	[REDACTED]	Lindell Cellphone 2	Voice (3 min 38 sec)
*2021-08-17 21:35:25 UTC	Lindell Cellphone 2	[REDACTED]	Voice (10 min 19 sec)
*2021-08-17 22:54:15 UTC	Lindell Cellphone 2	[REDACTED]	Voice (5 min 37 sec)

²⁴ Calls marked with an asterisk (*) reflect calls made between the [REDACTED] and telephone number [REDACTED] (“Lindell Cellphone 2”), which was not a number with which [REDACTED] had previously communicated (based on the call records currently in the government’s possession). Telephone number [REDACTED], however, is a cellular phone associated with MyPillow’s corporate Verizon Wireless account. Apple records also revealed that Lindell’s FaceTime usage was associated with two telephone numbers, the Lindell Cellphone (the primary number known to be used by Lindell) and [REDACTED]. Accordingly, investigators believe that the telephone number [REDACTED] is likely being used by Lindell.

T. [REDACTED] Recounted the Events at the Cyber Symposium

110. On August 18, 2021, links to a published video titled, “[REDACTED]” were posted on the website “https://www.resistancechicks.com,” as well as on the video streaming website Rumble at [REDACTED]. The posts were made by a user with the username “Resistance Chicks.” In the video, [REDACTED] discussed his experiences at the Cyber Symposium in front of a group called the Ohio Battleground Alliance. Investigators created the below unofficial transcripts from the recording.

111. In the video, [REDACTED] described the meeting he had in April 2021 in [REDACTED] office, during which [REDACTED] agreed to have [REDACTED] bring in a team to Mesa County to conduct a forensic audit:

After, I don’t know, an hour of this kind of discussion . . . and, it’s not, it’s not me like insulting her, right? I’m not saying you’re an evil person, you’re corrupting the nation. No. You know it’s like, you’ve been hacked, you just don’t know you’ve been hacked, okay. And we’re going through one at a time. Finally, she sent everybody out of the office and it’s just me, her, [REDACTED] and an attorney that we brought with us. And she’s like, okay, bring them in. So, we did a complete forensic audit of everything, all of her elections systems. Complete forensic audit of everything. You think Maricopa’s an audit? That’s peanuts. And you know what the difference is? She’s authorizing us to do this. She’s asking us to audit her systems because she believes there’s a problem. She’s doing her job as a real elections clerk. Yes, right? That’s what she should be doing. I’ve shown her evidence, she’s taking action. Brilliant. Got to love her. *But I remember saying, nobody can know about this. She said, if anybody finds out about this, it’s going to be bad.*²⁵ Because all the county clerks, they have this association, and they’re very tight, nobody breaks ranks. So of course, we protected her. But she’s not the only one.

²⁵ In this affidavit, italics in quoted language signify significant statements, rather than any emphasis by the speaker.

112. [REDACTED] described the actions of his team conducting a forensic audit, prior to and after the Mesa County Trusted Build in May 2021:

But what's really happening is that [Dominion is] coming in and wiping the systems. They're covering up all the past. How do we know? We have the image before and after they did the update. Because we, *when we sent our guys in to help her do a forensic audit, they stuck around for a couple of days.* Because what was happening was, they were having an election. So, we sent our guys in, we did a forensic audit. Dominion came in to program the machines for the new election. We did a forensic audit.

113. [REDACTED] described [REDACTED] involvement at Mike Lindell's Cyber Symposium on August 10, 2021:

So, um, [REDACTED] came out, Tuesday [August 10, 2021]. She announced [as] a whistleblower. Mike flew his jet down there, picked her up, and brought her to the cyber symposium and we announced it. It was a big announcement.

114. [REDACTED] described the struggle that Lindell's team of cyber experts had on August 9, 2021, on the eve of Mike Lindell's Cyber Symposium:

So here we are on Monday night [August 9, 2021]. It's Monday night, it's 11:00, the symposium starts 9:00 the next morning. We barely have any of the PCAPs [packet captures] that we're supposed to give to the guys the next day. We've got a program planned for the front so that we could have a show everybody can see. But we're about to have seventy guys in the back room who don't have anything to look at. And they are going to come out and say, all this PCAP stuff, we're out of here, this is bonk. Right? That's what we're facing.

...

So we're sitting there, what are we going to do? What are we going to do? And we started discussing, we are going to get Mr. Lindell in this room and we're going to tell him to write a check to all those guys to pay for their plane tickets and hotels and send them home. That is what we were doing in the room at 11:00 on Monday night. Because we were like, we're in trouble, we, this is all imploding.

...

So we're all, we're working on that strategy, we're trying to figure out what to do. You know, it's like ten of us in the room, computers everywhere. And, uh, [REDACTED] [likely [REDACTED], an attorney for

Lindell] phone rings. It's [REDACTED] from Mesa County. I want to come out tomorrow. I want to announce tomorrow. Suddenly, we go, and we have the forensic images! So imagine that you are mining for gold and as you are mining for gold you discover a diamond mine. That's exactly how we felt at that moment. Because forensic images are complete logs of everything. PCAPs are little snippets along the way, where you just capture this, capture that. It's like you're watching a security footage, you know, how you have a picture, then a picture, and a few seconds later there's another picture. They're not continuous. How would you like to have a complete log?

...

And it's even more powerful than that because we also have the source code for those machines, which nobody knew before we announced it. And, also, think about it. If you're writing computer software, you don't write separate software for every machine. Right? You write it, it goes on all of the machines. Guess what? All of the instructions that work on all the other machines around the country, and all the access codes, and all that Internet access, where to do this and how to do that, it's all in there. Right? So once you have, like, one complete set, you are really set up.

115. [REDACTED] described [REDACTED] as having "chickened out" at Mike Lindell's Cyber Symposium the evening of August 10, 2021, and Lindell offered to pay for lawyers for [REDACTED] and to protect and hide [REDACTED] if she would speak at the event:

What was supposed to happen [on Tuesday] when [REDACTED] came out was that we were supposed to announce we also have the forensic images of Mesa [County] and also that we had [forensic images from a Michigan county's election system] as well. We didn't get to that because at the last-minute [REDACTED] chickened out.

...

Lindell is in the back room saying, whatever you need I'm going to give it to you. You need lawyers, I'm going to give it to you. If you need to be hidden, I'm going to hide you around the country. Whatever you need. She's afraid. You know why she's afraid? They raided her office that day.

And her colleague [likely referring to [REDACTED]], they raided his house and took all of the electronics out of his house including his children's. He has four small children. They took all of their electronic toys. They just, this is intimidation. This is not investigation. This is, you cross us, we're coming after you. That is not democracy. That's not the America I grew up in. I'm getting

mad now. Can you see I'm getting worked up here? You don't take my children's toys away. These people are . . . these people are evil. Okay. This is good and evil now. Okay. This is not about let's have a legal process and let's have legal investigations. This is about, I am going to intimidate you, if you've crossed the line, if you come public, we are going to punish you.

116. [REDACTED] described his role on August 11, 2021, at Mike Lindell's Cyber Symposium:

Wednesday morning [August 11, 2021], my job is to sit there for four hours live on [Lindell's website [REDACTED]], explaining the before and after images from Mesa County to the world so that they can understand what they are seeing. So, it's the first time that I've seen them. I was supposed to be looking at this, understanding everything that's happening. Good thing that I speak geek. So, I'm watching this and we got famous hackers on the screens, we got famous hackers on the stage. And I'm supposed to be listening, watching, contributing, participating with the hackers in the audience who were like amazing cyber guys.

117. A review of all call records obtained in this investigation between the [REDACTED] and the Lindell Cellphone revealed that the two parties exchanged approximately 252 voice calls and 214 text messages between April 7, 2021, and April 5, 2022.

U. [REDACTED] Linked to [REDACTED] via the Antrim County Forensic Images

118. [REDACTED] is a resident of Florida who is the former CEO of [REDACTED]. Like Lindell, [REDACTED] has persistently made public assertions that widespread election fraud occurred in the 2020 presidential election. Also like Lindell, [REDACTED] has promoted claims that Dominion election computers were deliberately designed to rig the results of the 2020 presidential election. [REDACTED] is also a leader of an election integrity group known as [REDACTED]. The group was reported to be one of the largest funders of an election audit that

took place in Arizona's Maricopa County in 2021. By July 2021, the Associated Press reported that [REDACTED] had contributed \$3.25 million for the Maricopa County election audit.²⁶

119. On or about August 10, 2021, the same day as the start of Lindell's Cyber Symposium, Dominion filed a \$1.6 billion dollar defamation lawsuit alleging that [REDACTED] had made false claims about how Dominion's voting machines were manipulated to rig the 2020 election against President Donald Trump. *See* Case No. 1:21-CV-02130 (D.D.C.), ECF No. 1 (Complaint).

120. As described in an investigative report published by news organization ProPublica on [REDACTED],²⁷ [REDACTED] and [REDACTED] have been linked to an effort to obtain forensic disk images of election computers in Antrim County, Michigan, in December 2020. ProPublica reported that [REDACTED] had paid for [REDACTED] to travel by private plane to Antrim County to conduct an analysis of Antrim's election computers. [REDACTED] also spoke to ProPublica about his role in that effort, explaining that he had drafted an initial version of a report on the analysis.

V. [REDACTED] Indirectly Revealed that [REDACTED] Recorded and Retained Cell Phone Video Taken at the Mesa County Trusted Build in May 2021

121. On or about March 23, 2022, [REDACTED] distributed a video from his website at "[REDACTED]" In the video, [REDACTED] described [REDACTED] as bringing in "a computer scientist, a white hat hacker, a licensed guy" (as discussed throughout this affidavit, this individual was likely [REDACTED]) to make forensic images of Mesa County's election computers in May 2021:

Dirty politicians around the country started worrying about Maricopa [County, Arizona-like election] audits happening in their counties and their states. And they started preparing. And the

²⁶ *See* [REDACTED]

²⁷ *See* [REDACTED]

Secretary of State of Colorado, Jena Griswold, who's dirty . . . made arrangements and said, Dominion is going to come in and wipe your, well, no, said they would just touch this little part of the machine that's the application that has their software on it. They were not going to touch the other stuff. Well, [REDACTED], Mesa County Colorado, says, I'm not sure I believe that. I'm not sure anyone should be in here fiddling with these machines.

...

And [REDACTED]s] caused a computer scientist, a white hat hacker, a licensed guy who can give court testimony and affidavits, very high-end, white hat security guy. Works for the government all the time, has done all kind of projects for them, he can write affidavits that show up and [are] used in hundreds of court cases. Things like this. [REDACTED] got this fellow in. What's funny is he happens to be a bad ass. He's a real bad ass. I'm not going to tell you anything more. He's a bad ass but he is an unassuming bad ass. And he went in, and, you know, got some, *they gave him some county credentials or something, and he dressed up like a little nerd.* And he went in. And he took an image, a forensic image that can be producible in court. That's what he does. A forensic image of the hard drive on the election equipment as it existed at the county before the guys with their trusted build showed up.

122. [REDACTED] described the "outside, court-certified, cyber guy" having used his Apple iPhone during the Mesa County Trusted Build to communicate with [REDACTED] via FaceTime (a video chat program) as well as to make video recordings of Dominion and Colorado Secretary of State employees:

Then the guys with the trusted build showed up. And what is funny then, and unbeknownst to them, the fellow sitting next to them, one of the county workers, while Dominion and the Secretary of State, I believe, had her own people in there with Dominion to do this trusted build . . . unbeknownst to them, one of those county workers wasn't really a county worker. One of those county workers was this outside, court-certified, cyber guy who was keeping an eye on them. He actually called me from the middle . . . he was sitting next to them at one point that day. This was back I think in May or June of last year. He actually called me on FaceTime and he sat there telling me, I can't believe what I'm seeing. I'm seeing these people commit a million felonies right next to me, and I'm just watching them. And he had the FaceTime up so I can see the people doing what they were doing. And he also took some videos of them doing what they were doing. [What they were doing] was highly illegal. They were wiping

out, they wiped out, the entire hard drive that contained the 2020 election, so it could never be verified, it could never be audited now.²⁸ That's one thing they did. And they installed on top of it, their new build. So, when they were gone, [the outside cyber guy] then went and got a forensic image of that build of that hard drive. A forensic image means a perfect bit-by-bit copy. Then, those two things were sent, so t— . . . uhhh, those things were sent to some computer scientists.

123. [REDACTED] described the “outside, court-certified, cyber guy” having assumed another identity to appear as a legitimate Mesa County employee while video recording the Mesa County Trusted Build:

[The outside cyber guy] had a name like [REDACTED] or something on his name tag. [REDACTED] the county worker. Hey, message to Dominion and Colorado Secretary of State. *That guy with [REDACTED] on his name tag, next to you, he was actually one of ours.* He was filming you fuckers. *[Laughs, slaps desk.]* He was filming you fuckers.

...

And those two reports, those two images, the hard drive, went out to these high-end computer science professionals who are now working for the [REDACTED] defense team. Why does she need a defense team? Because when the Colorado Secretary of State found out what she did, she sicced the authorities on [REDACTED]. [REDACTED], who is just trying to do her job and caught this crook. That crook has now gotten her indicted because she let someone else into the Colorado, she let someone else on the machines, she let somebody, you know, all this kind of stuff.

124. [REDACTED] explained that the “outside, court-certified, cyber guy” retained copies of the video recordings of the Mesa County Trusted Build taken with his cellphone:

Incidentally, this [outside cyber guy] who I describe. The guy who got all buttoned up and posed as a little, wimpy computer guy, and did all this filming, [who] sat next to the Dominion guys and filmed them when they came in and played with the machines. [The outside cyber guy] has the films of them, incidentally, of them doing this. Maybe I shouldn't be letting that...

²⁸ The Trusted Build merely updated the Dominion computer system. Paper ballots from the 2020 election at all times remained available for any potential audit. This was also confirmed by Mesa County Deputy Clerk [REDACTED] in her June 2022 interview with investigators.

...

It just will be interesting if they deny, I don't know how they could deny, this is all black and white now, but if they were to deny it, there was actually a county worker there who was with them who was on his phone a lot, he was actually filming them. Just so you guys know. [REDACTED], just so you know, your people were being filmed while they were in there doing [inaudible] with the computer. Ha. Ha. Ha.

125. [REDACTED] explained his support for [REDACTED] and her actions as follows: "desperate times call for desperate measures."

So, now, in the bizarro world we live in, the Secretary of State got that Country Recorder [REDACTED] arrested. Got her on 10 indictments. And she is looking at 10 indictments for things like, you know, letting someone else make a copy of the hard drive. And letting someone else enter the room who wasn't really a County Recorder, or you know, county computer . . . well, desperate times call for desperate measures. Her job was protecting the integrity of the data, the records of Mesa [County] Colorado, and to protect the . . . that's what the County Recorder does, and she did something, you know, she had something a little unusual thrown at her and she took a little unusual step herself.

W. [REDACTED] Charged By State and Local Officials in Colorado

126. In March 2022, the 21st Judicial District Attorney's Office in Colorado obtained an indictment from a Colorado grand jury against [REDACTED] and [REDACTED], alleging that [REDACTED] committed a series of crimes under Colorado law in connection with the above-described events. That case is now pending in Colorado state court in Grand Junction, Colorado. In addition, [REDACTED] has been charged with burglary and cybercrime for entering the Mesa County Clerk and Recorder's office and attempting to access a county computer after she had been placed on administrative leave. In late August 2022, she pled guilty to lesser charges and agreed to cooperate in the prosecution of [REDACTED]. [REDACTED] has also been issued a contempt citation for allegedly

recording, without authorization, a recent court hearing in Mesa County.²⁹ Finally, [REDACTED] has been charged in Colorado state court with conspiracy to commit criminal impersonation and attempting to influence a public servant.

X. Ongoing Communications Between Mike Lindell and [REDACTED] from February 24, 2021, to June 28, 2022

127. Lindell and [REDACTED] have apparently continued to engage in regular communication since the events described in this affidavit.

128. Records of incoming and outgoing telephone calls and SMS text messages obtained from T-Mobile USA and Verizon Wireless revealed that from February 24, 2021, to June 28, 2022, the [REDACTED] and the Lindell Cellphone communicated approximately 1,088 times. The last record of a communication obtained by investigators occurred on June 27, 2022, at 21:00 UTC, the date of the most recent records request.

Y. Mike Lindell Paid At Least \$878,000 to [REDACTED] between May 10, 2021, and April 8, 2022

129. Bank records obtained by investigators for a personal account associated with [REDACTED] revealed that between May 10, 2021, and April 8, 2022, [REDACTED] received 11 wire transfers from Lindell Management LLC for a total amount of \$878,076.12 (including the three wire transfers described above from May 2021, July 2021, and August 2021).

²⁹ In February 2022, Mesa County investigators obtained a warrant to seize an iPad belonging to [REDACTED]. The purpose of the seizure was to obtain evidence related to the contempt citation. During the execution of the warrant, [REDACTED] attempted to kick one of the officers assisting with the warrant execution. A separate misdemeanor case is pending against her related to this conduct.

Z. Mike Lindell Makes Public Statements Linking His Ongoing Litigation Against Dominion to the Mesa County Incident.

130. On March 23, 2022, Lindell and [REDACTED] appeared as [REDACTED] guests on the [REDACTED] show,³⁰ which was streamed on Lindell's FrankSpeech website.³¹ The following is an unofficial transcript of parts of the discussion. During this conversation, Lindell drew an explicit link between obtaining the contents of Mesa County's voting machines and his ongoing litigation against Dominion. Lindell also referenced a report issued by [REDACTED] defense team that purported to advance the theory that the Mesa County voting machines were vulnerable to manipulation.

Lindell: [A forensic report analyzing the Mesa County election server disk images and published by [REDACTED] defense team is] going to vindicate both [REDACTED] and myself.

...

Lindell: I'm excited because it's [now been] vindicated. . . . It's here. It's over. These guys are guilty.

...

Lindell: Read the report. Understand what went on. What took months to get to this point. . . . It's over. Dominion, you're guilty. Machines cannot be used in this next election. And you know what? Every lawsuit in this country should go away today because it's over. They're caught.

...

[REDACTED] This is my point. If what these technicians say, and the people who checked it, is true, you would surmise that all these suits that Dominion has against everybody would go away. Is that the case you are making? You think you've got the smoking gun that shows that Dominion actually did this. There are no more assertions. You've got the receipts. And if these receipts are real, [that] cuts out the underpinnings of all the Dominion . . . this is what your position is?

Lindell: Absolutely, [REDACTED] . . . And not just only should all these lawsuits go away, but we are going to start with preliminary

³⁰ [REDACTED].

³¹ See <https://frankspeech.com/video/mike-lindell-i-have-receipts-stolen-election>.

injunctions because now it makes it very easy to go state-by-state . . . for them not to use any computers, any machines, in our 2022 elections. . . . No machines. No computers. No electronic polling book. Nothing. Because now we have definitive proof. Definitive proof. No one in the world can deny this now, [REDACTED]. No one.

...

Lindell: [This latest [REDACTED] defense report] is the biggest breaking news, bombshell proof. We finally have what's inside the machine. . . . We're on offense, [REDACTED] I have been on offense, you know that. I don't go to defense. This is what I've had all along. . . . It's over, everybody. If we can get the word out to the world, it's over.

...

[REDACTED] Just a yes or no answer. Do you believe this evidence you put out in this third report totally makes the case that the machines were the problem? Yes or no.

Lindell: A hundred percent. Over. Well, there's other things too, mail-in votes, but a hundred percent that they manipulated our election and stole our election.

AA. "Damage" to the CVM as defined by 18 U.S.C. § 1030(e)(8)

131. There is probable cause to believe that the changes made to the Mesa County CVM's BIOS settings during or reasonably near the time of the surreptitious forensic imaging in May 2021—disabling Secure Boot and allowing the computer to boot from the Optical Drive—damaged the CVM. As noted, damage includes “any impairment to the integrity . . . of data, a program, a system, or information.” 18 U.S.C. § 1030(e)(8). Based on my training and experience, as well as my conversations with other FBI personnel, disabling Secure Boot increases the risk that malware can be introduced and run undetected on a computer. Enabling Optical-Drive boot may also impair the integrity of a computer and the data on it. The Optical-Drive boot setting allows a person to run an Operating System from a CD or DVD, bypassing the computer's internal Operating System drive in the process. At that point, a malicious actor could install malware or navigate to the computer's internal Operating System drive and add, edit, or delete data—all

without leaving noticeable evidence of their activities. In part for that these reasons, the Colorado Secretary of State de-certified the Mesa County CVM and prohibited it from being used in future elections; the Secretary of State explained that it could not “establish confidence in [the Mesa County CVM’s] integrity or security.”

132. As noted: (i) the CVM is designed to be a “closed” system, to protect it from outside interference; (ii) only the Colorado Secretary of State’s Office should possess the CVM’s BIOS passwords—not the Mesa County Clerk and Recorder’s Office or any other entity; (iii) nonetheless, BIOS settings for the CVM were reportedly changed, a modification that required use of the BIOS passwords and one that affected the integrity of the system and the data on it; (iv) ██████ admitted that she directed copying of the CVM before and after the Trusted Build; and (v) key card access logs place ██████ ██████ (likely ██████), and ██████ in the Elections Office on the days the CVM was imaged. And for the reasons articulated throughout this affidavit, there is probable cause to believe that evidence relevant to the damage to the CVM will be found on the ██████, the Lindell Cellphone, and the ██████.

BB. Seizure of Certain Electronic Devices

133. As indicated above, investigators for the 21st Judicial District Attorney’s Office have executed numerous search warrants, including at the Mesa County Clerk and Recorder’s Office and the home of ██████.

134. On August 11, 2021, investigators for the 21st Judicial District Attorney’s Office executed a search warrant issued by Colorado 21st Judicial District Court Judge Valerie J. Robison, under docket number ██████, at the ██████ residence, located at ██████. ██████ was not at home during the execution of the warrant. According to messages obtained from ██████ cell phone (on an end-to-end encrypted messaging

platform called Signal), which was obtained pursuant to the search warrant described in the following paragraph, [REDACTED] was at the Lindell symposium on August 11, 2021. The execution of this warrant resulted in the seizure of 22 electronic storage devices, including but not limited to Apple iPads, cellular telephones, external hard drives, and optical disks.

135. On September 3, 2021, the FBI obtained federal search warrants issued by the Honorable Nina Y. Wang, U.S. Magistrate Judge for the District of Colorado, under docket number [REDACTED], to search 16 of the 22 devices that had already been seized by Colorado law enforcement. These warrants were executed shortly thereafter, and analysis of these 16 devices is in progress.

136. On August 16, 2021, investigators for the 21st Judicial District Attorney's Office executed a search warrant issued by Colorado 21st Judicial District Court Judge Valerie J. Robison, under docket number [REDACTED], at the Mesa County Clerk and Recorder's Office. It was during the execution of this warrant that 21st Judicial District Attorney's Office investigators seized the CVM. On September 29, 2021, the FBI obtained search warrants issued by the Honorable Gordon P. Gallagher, U.S. Magistrate Judge for the District of Colorado, under docket number [REDACTED], to search these already-seized devices. These warrants were executed shortly thereafter, and analysis of the CVM also remains in progress.

137. On August 23, 2021, 21st Judicial District Attorney's Office investigators obtained an additional search warrant issued by Colorado 21st Judicial District Court Judge Richard T. Gurley, under docket number [REDACTED], to seize numerous electronic devices at the Mesa County Clerk and Recorder's Office. Investigators for the 21st Judicial District Attorney's Office executed this warrant over two different days, between August 23 and 24, 2021. Over the course of these two days, investigators seized multiple electronic devices issued by Mesa County to

individuals of interest in this investigation. As relevant here, the execution of this warrant resulted in the seizure of an Apple iPhone XR issued to [REDACTED], a Dell laptop issued to [REDACTED], a Dell laptop issued to [REDACTED], and a USB storage device found on the desk of [REDACTED]. The execution of this warrant also resulted in the seizure of data from Mesa County network folders assigned to [REDACTED]. Review of this data is ongoing.

138. On August 26, 2021, investigators for the 21st Judicial District Attorney's Office executed an additional search warrant issued by Colorado 21st Judicial District Court Judge Richard T. Gurley, under docket number [REDACTED], to seize [REDACTED] Mesa County-issued computer from the Mesa County Clerk and Recorder's Office.

139. On October 6, 2021, the FBI obtained search warrants issued by the Honorable Gordon P. Gallagher, U.S. Magistrate Judge for the District of Colorado, under docket number [REDACTED], to search the various non-CVM devices from the Mesa County Clerk and Recorder's Office, as well as a separate Blu-Ray disc containing an extraction of the data contained on [REDACTED] County-issued cell phone. Analysis of these devices is in progress.

140. On November 13, 2021, District of Colorado U.S. Magistrate Judge Gallagher issued four search warrants for the residences and persons of [REDACTED], [REDACTED], and [REDACTED], under docket number [REDACTED]. These warrants were executed on November 16, 2021. As a result of these warrants, the FBI seized numerous digital devices belonging to these four individuals. These devices are currently undergoing a review by a filter team to avoid exposing the investigative team to any attorney-client communications. As a result, the investigative team has only been able to review a small portion of these devices' contents to date. Below is a list of certain devices seized from each of the four locations:

Location	Seized Digital Devices
[REDACTED]	White iPhone Black TCL Phone, Rose iPhone, WD MyPassport, Lacie External HD, Black iPhone SE, Black iPhone 7, Black iPhone 7, Compaq Laptop, HP Laptop, and MacBook
[REDACTED]	Samsung Cell, Motorola Cell, LG Tablet, HP Laptop, and ASUS Laptop
[REDACTED]	Samsung Cell, HP Laptop Lenovo
[REDACTED]	Samsung Cell, iPhone, Blu Phone, HP Desktop, Loose HD, ASUS Laptop, and MSI Laptop

CC. Encrypted Communications Applications on [REDACTED] and Lindell's Mobile Devices

141. Records received from Apple indicate that both [REDACTED] and Lindell had multiple end-to-end encrypted messaging applications installed on their Apple devices during the investigative review period from October 2020 to April 2022, including Signal, Telegram, WhatsApp, and Wickr. These applications allow the exchange of encrypted text messages between users of electronic devices in a manner ensuring that a third party, such as a cell phone service provider or information technology company, cannot obtain the content of the messages. Users of these applications may retain messages for a lengthy period of time on a particular device, or they

may choose settings that either retain the messages for a short period of time (such as one week) or automatically “auto-destruct” each message.³²

142. The table below is a summary of the encrypted messaging applications installed on various mobile devices belonging to Lindell and [REDACTED]. The data in the table establishes that Lindell and [REDACTED] have downloaded multiple encrypted messaging applications onto the Lindell Cellphone and the [REDACTED]. The information in this table was drawn from a combination of records produced by Apple, Verizon, and T-Mobile, in response to various legal process. These records indicate, from the first to the last column: (a) the user and Apple ID (Lindell appears to have two separate Apple IDs); (b) the encrypted messaging application downloaded by that user; (c) the date range of software updates (made via Apple’s App Store) to the particular encrypted messaging applications; (d) the physical device associated with the particular Apple ID in Apple records; and (e) the physical device and phone number associated with the subscriber in Verizon and T-Mobile records.

³² For example, Signal advertises that “anyone” in a chat can turn on “disappearing messages.” Each disappearing message has a timer that is visible at the bottom of the message. Any changes to the timer will automatically sync between the user’s linked devices. Once the timer ends, the message is deleted. Signal states that it offers disappearing messages so users can “keep [their] message history tidy.” *See* <https://support.signal.org/hc/en-us/articles/360007320771-Set-and-manage-disappearing-messages>.

<u>Subscriber / Apple ID</u> <u>(Source: Apple records)</u>	<u>Mobile App</u> <u>(Source: Apple records)</u>	<u>Date Range of</u> <u>App Updates</u> <u>on Device</u> <u>(Source: Apple records)</u>	<u>Apple Device</u> <u>Version /</u> <u>Apple Device</u> <u>Family</u> <u>(Source: Apple records)</u>	<u>Mobile</u> <u>Provider</u> <u>Description /</u> <u>Telephone</u> <u>Number</u> <u>(Source: Verizon and T-Mobile records)</u>
[REDACTED]	Signal – Private Messenger	11/19/2020 – 4/5/2022	iPhone13,2 / iPhone 12	IPHONE 12 BLACK 128GB-USA / T-Mobile telephone [REDACTED] (i.e., the [REDACTED])
	Telegram Messenger	11/19/2020 – 3/12/2022		
Mike Lindell / [REDACTED]	Signal – Private Messenger	11/18/2020 – 3/14/2022	iPhone13,4 / iPhone 12 Pro Max	IPHONE 12 PRO MAX 512 / Verizon telephone [REDACTED] (i.e., the Lindell Cellphone)
	WhatsApp Messenger	11/18/2020 – 8/17/2021		
Mike Lindell / [REDACTED]	Wickr Pro / Wickr Me-Private Messenger	2/13/2021 – 8/17/2021		
	Telegram Messenger	7/7/2021 – 12/12/2021		

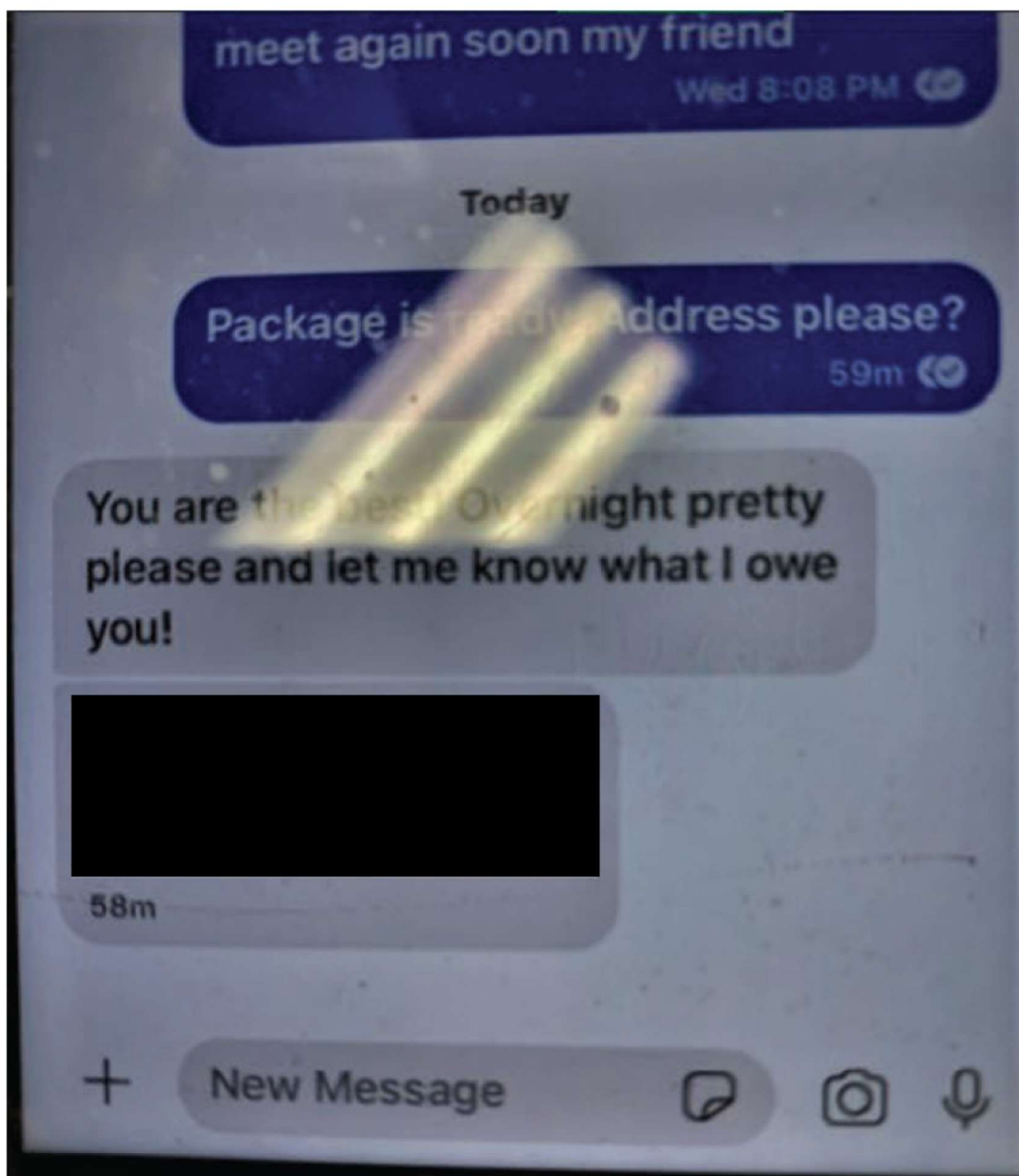
143. Communications sent over Signal (and perhaps other encrypted messaging applications) would not appear on call records obtained from a cellular service provider like Verizon or T-Mobile.

144. There is additional evidence that [REDACTED] and other co-conspirators communicated using end-to-end encrypted messaging. In particular, agents have obtained a photograph of [REDACTED] cell phone screen reflecting a series of messages over the Signal messaging platform between [REDACTED] and [REDACTED]. As described above, on May 27, 2021, [REDACTED] directed a subordinate

employee to mail a package to be addressed to [REDACTED]
[REDACTED]. This address is also listed in Apple records as one of the addresses associated with [REDACTED] iCloud account with the Apple ID [REDACTED]” [REDACTED] appears to have obtained this shipping address from [REDACTED] via a messaging platform, and then [REDACTED] displayed her cell phone screen—containing the address and a limited number of additional messages between [REDACTED] and [REDACTED]—to the employee so that the employee could take a photograph of the screen and ship the package to the correct address.

145. The employee took the following photo of what was partially displayed on [REDACTED]

[REDACTED] screen:



146. Through training and experience, investigators recognize the white checkmark read-receipts in these communications as an indicator that the messages were sent over the Signal messaging application. The subordinate employee reported her understanding that [REDACTED] was at that time communicating with the person to whom [REDACTED] had directed the employee to send the package to, *i.e.*, [REDACTED].

147. The metadata of the employee's photo indicated that it was taken on May 27, 2021, at 18:17 UTC (or 12:17 p.m. Mountain Time), which is the date on which the second image of the Mesa County CVM appears to have been completed. The last text message shown in the photo indicated that it was delivered 58 minutes prior. Therefore, it can be inferred—based on the interview with the employee, the photograph, and the metadata associated with the photograph—that [REDACTED] was communicating with [REDACTED] via the Signal application between approximately 11:19 a.m. and 12:17 p.m. Mountain Time.

148. The call detail records provided by Verizon for [REDACTED] cell phone reflect no text message communications with the [REDACTED] or any other cellphone at or around this time. This is consistent with how investigators understand encrypted messaging applications like Signal operate; such messages in their original form can generally only be viewed on the physical cell phone devices from which they were sent or received.

149. There is also evidence that [REDACTED] has shifted her communications to end-to-end encrypted messaging platforms due in part to the investigation into the data breach described throughout this affidavit. According to an interview conducted by law enforcement with Mesa County Commissioner [REDACTED], [REDACTED] informed [REDACTED] on August 9, 2021—the day that the Colorado Secretary of State issued an order prohibiting [REDACTED] from accessing Mesa County voting machines without the written permission of the Secretary, as described above—that [REDACTED] could communicate with [REDACTED] using Signal.³³ [REDACTED] stated that she has been a friend of [REDACTED] for approximately four years and has communicated regularly with [REDACTED]

³³ According to [REDACTED] [REDACTED] had asked [REDACTED] if she was available to take a walk with [REDACTED] and [REDACTED]. In substance, [REDACTED] was asking [REDACTED] if she was available to discuss a matter with [REDACTED] and [REDACTED] in person, as opposed to via text message or over the telephone.

through cell phones without using encryption technology; before this incident, [REDACTED] had never sought to communicate with [REDACTED] through Signal. Again, investigators know from training and experience that Signal data and content can be stored on cell phones themselves and can sometimes be extracted through forensic tools and software.

150. Similarly, a review of a portion of an iPhone seized from [REDACTED] residence on November 16, 2021—and which has cleared the filter review process—contains additional discussion about the use of Signal. Specifically, in a text message conversation from November 1, 2021, between [REDACTED] and [REDACTED] [REDACTED] observed, in substance, that she was receiving negative media coverage. [REDACTED] then stated, “More but I’d rather talk by signal.” On November 8, 2021, in a text message conversation on the same mobile device between [REDACTED] and [REDACTED] [REDACTED] informed [REDACTED] in substance, that [REDACTED] was going to someone named “[REDACTED]” about “the plan.” [REDACTED] then added, “I’ll fill you in when we talk by signal.”

DD. Summary

151. Based on my training and experience as an FBI Special Agent, my conversations with other law enforcement personnel, and my everyday experience, I know that individuals make pervasive use of cellphones to communicate with one another, manage aspects of their personal lives, obtain information over the Internet, and perform work functions such as drafting and storing documents and records. I also know from my everyday experience that individuals tend to carry their cellphones on their persons or keep them in the immediate vicinity of their persons. The use of encrypted messaging platforms such as Signal, as outlined above, makes it difficult for law enforcement to gain access to communications among the individuals discussed above without gaining possession of the actual electronic devices where these communications are stored.

152. Likewise, applications like Apple's iCloud service—available on any iPhone—allow a user to access files originally created or received on one Apple device from another device. I also know from my training and experience as an FBI Special Agent and my everyday experience that it is a common practice for individuals to carry over a substantial amount of electronic data from one cell phone to another when, for instance, an individual upgrades his/her cellphone to a different model but retains the same telephone number. In this regard, applications, text messaging history, emails, contacts, and other information will frequently be carried over from one cellphone handset to another. Thus, even if [REDACTED], or Lindell were to obtain a new cell phone handset different from the one used to communicate in 2021, there is still probable cause to believe that evidence of the SUBJECT OFFENSES would be found on that new cellphone.

153. As set forth above, there is probable cause to search the person of Mike Lindell for the Lindell Cellphone, and to seize and search the Lindell Cellphone for the items described in Attachment B. By way of a non-exhaustive summary, Lindell has made numerous public statements about his interest in finding information that undermines the integrity of the November 2020 election, with a particular focus on Dominion voting machines such as the ones in Mesa County. Lindell has a personal financial motive to find evidence undermining the integrity of Dominion machines, as he is facing substantial litigation from Dominion based on Lindell's disparaging statements about the machines. Lindell's extensive telephonic communications with [REDACTED] and his significant payments to [REDACTED] throughout 2021, including at or around the same time as the key events in Lake and Mesa Counties, indicate that Lindell knew about and supported the infiltration of the Trusted Build in Mesa County by [REDACTED]. Lindell's extensive public statements and financial support for [REDACTED] and his sponsoring of the August 2021 symposium

where information obtained from Mesa County was presented further implicates Lindell in the SUBJECT OFFENSES.

154. Lindell's apparent use of encrypted messaging applications, and his extensive telephonic and text message communications with [REDACTED] using the Lindell Cellphone demonstrate that there is probable cause to believe that evidence of the SUBJECT OFFENSES will be found on the Lindell Cellphone

TECHNICAL TERMS

155. Based on my training and experience, as well as my conversations with other FBI personnel, I use the following technical terms to convey the following meanings:

- a. BIOS: The Basic Input/Output System, or BIOS, is firmware used to perform hardware initialization during the booting process (power-on startup). The BIOS firmware comes pre-installed on a computer's system board, and it is the first software to run when powered on. A BIOS may be secured with a password to restrict access to the BIOS user interface and to prevent users from changing settings such as enabling or disabling the ability to boot a system from portable storage devices.
- b. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

- c. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- d. “Electronic storage medium” means any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.
- e. In this affidavit, the terms “computers” or “digital storage media” or “electronic storage medium” or “digital storage devices” may be used interchangeably, and are intended to include all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices capable of performing logical, arithmetic, or storage functions, any physical object upon which computer data can be recorded, including desktop and laptop computers, computer hardware, computer software, volatile data, cellular telephones, tablets, server computers, gaming devices, network hardware, hard disk drives, RAM, floppy disks, flash memory, CDs, DVDs, and other magnetic or optical storage media, as well as computer related documentation, computer passwords and data security devices, digital communications devices, cameras, videotapes, video recording devices, video recording players, and video display monitors, digital input and output devices such as keyboards, mouse(s), scanners, printers, monitors, electronic media and network equipment, modems, routers, connection and power cords, and external or connected devices used for accessing computer storage media that was used to

commit or facilitate commissions of the SUBJECT OFFENSES (collectively herein, “computers”).

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

156. As described above and in Attachment B, this Affidavit and associated application seeks permission to seize and search the Lindell Cellphone for evidence of the SUBJECT OFFENSES. This evidence would include data stored on the cellphone’s hard drive. Thus, the applied-for warrant would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

157. *Probable cause.* I submit that if the Lindell Cellphone is successfully located and seized, there is probable cause to believe that evidence of the SUBJECT OFFENSES will be stored on the cellphone, for at least the following reasons in addition to those articulated throughout this affidavit:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition,

a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

- c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

158. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the cellphone was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be stored on the electronic storage medium, *i.e.*, the Lindell Cellphone, for the following reasons:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail

programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner.
- c. Further, computer and storage media activity can indicate how and when the computer or electronic storage media was accessed or used. For example, as described herein, computers typically contain information that logs computer user

account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation.

- d. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and suspects. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (*e.g.*, a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (*e.g.*, Internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- e. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- f. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- g. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

159. *Necessity of seizing or copying entire electronic storage media.* In most cases, a thorough search for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from an individual's possession, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or

imaging is often necessary to ensure the accuracy and completeness of data recorded on the electronic storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on the location where the device might be seized could be unreasonable. As explained above, because the warrant calls for the seizure of forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine electronic storage media to obtain evidence. Electronic storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt during a physical seizure.
- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present at the time, and in the location where, the warrant is executed. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data at the time of the seizure. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.
- d. Volatile data. Based on my knowledge, training, and experience, I know that a powered-on computer maintains volatile data. Volatile data can be defined as active information temporarily reflecting a computer's current state including registers, caches, physical and virtual memory, network connections, network shares, running processes, and printing activity. Collected volatile data may contain such information as opened files, connections to other computers, passwords used for encryption, the presence of anti-forensic tools, or the presence of programs loaded in memory that would otherwise go unnoticed. Volatile data and its corresponding evidentiary value are lost when a computer is powered-off.

160. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying the Lindell Cellphone, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrants.

161. *Use of Biometric Features to Unlock Electronic Devices.* The warrant I am applying for would permit law enforcement to obtain from Michael Lindell the display of physical biometric characteristics (such as fingerprint, thumbprint, or facial characteristics) in order to unlock devices subject to search and seizure pursuant to this warrant. I seek this authority based on the following:

- a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners and facial recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.
- b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called “Touch ID,” which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device’s Touch ID sensor, which is found in the round button (often referred to as the “home” button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.
- c. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face or iris. For example, Apple offers a facial recognition feature called “Face ID.” During the Face ID registration process, the user holds the device in front of his or her face. The device’s camera then analyzes and records data based on the user’s facial characteristics. The device can then be unlocked if the camera detects a face with characteristics that match

those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Face ID.

- d. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.
- e. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 4 hours *and* the passcode or password has not been entered in the last 156 hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.
- f. Due to the foregoing, if law enforcement personnel determine that the Lindell Cellphone may be unlocked using one of the aforementioned biometric features,

the warrant I am applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of Michael Lindell to the fingerprint scanner of the device; or (2) hold the device in front of the face of Michael Lindell and activate the facial recognition feature, for the purpose of attempting to unlock the Lindell Cellphone in order to search its contents as authorized by this warrant.

162. The proposed warrant does not authorize law enforcement to require that Lindell or any other individual state or otherwise provide the passcode, or identify specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access any electronic devices. Nor does the proposed warrant authorize law enforcement to use the fact that the warrant allows law enforcement to obtain the display of any biometric characteristics to compel the aforementioned persons to state or otherwise provide that information. However, the voluntary disclosure of such information by Lindell (or others) would be permitted under the proposed warrant. To avoid confusion on that point, if agents in executing the warrant ask Lindell for the passcode to any electronic device, or to identify which biometric characteristic (including the unique finger(s) or other physical features) unlocks any electronic devices, the agents will not state or otherwise imply that the warrant requires Lindell to provide such information, and will make clear that providing any such information is voluntary and that Lindell is free to refuse the request.

ATTORNEY COMMUNICATIONS

163. If the government becomes aware of a reasonable possibility that seized materials may include attorney-client privileged information, the government will implement filter protocols to safeguard attorney-client privileged materials and segregate those materials from review by any member of the investigative team.

REQUEST FOR SEALING

164. It is respectfully requested that this Court seal this warrant until further order of the Court, including all papers, such as the application and affidavit, submitted in support of the warrant. I believe that restricting these documents is necessary because the warrant is relevant to an ongoing investigation into the SUBJECT OFFENSES, and not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that perpetrators actively search for criminal affidavits and search warrants via the Internet and disseminate them to other co-conspirators and criminals as they deem appropriate. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

CONCLUSION

165. I submit that this affidavit supports probable cause for a search warrant authorizing the search of Michael Lindell, described in Attachment A, for the items described in Attachment B (including the Lindell Cellphone).

Respectfully submitted,



J. A. Myszkiwicz
Special Agent
Federal Bureau of Investigation

SUBSCRIBED and SWORN before me by reliable electronic means (FaceTime, Zoom and/or email) pursuant to Fed. R. Crim. P. 41(d)(3) on September 7th, 2022



The Honorable Tony N. Leung
United States Magistrate Judge

ATTACHMENT A
Location to Be Searched

The property to be searched is the person Michael James LINDELL (“LINDELL”)—a male [REDACTED], approximately 6 feet tall, with social security number ending in [REDACTED]—and any items on his person or in his immediate control in which the LINDELL CELLPHONE (as defined in Attachment B) could reasonably be found. A photograph of LINDELL appears below:



ATTACHMENT B
Items to Be Seized

1. The physical cellular telephone assigned call number [REDACTED] (the “LINDELL CELLPHONE”); and

2. All records and information on the **LINDELL CELLPHONE** that constitute fruits, evidence, or instrumentalities of violations of 18 U.S.C. §§ 1028(a)(7) (identity theft), 1030(a)(5)(A) (intentional damage to a protected computer), and/or 371 (conspiracy to commit identity theft and/or to cause intentional damage to a protected computer)—(the “SUBJECT OFFENSES”)—those violations involving [REDACTED]
[REDACTED], Michael Lindell, and/or [REDACTED], among other co-conspirators known and unknown to the government (the “SUBJECTS”), since November 1, 2020, including:

- a. All records and information relating to damage to any Dominion computerized voting system, including any impairment to, or attempt to impair, the integrity or availability of data, a program, a system, or information;
- b. All records and information relating to BIOS on any Dominion computerized voting system, including any modification to, or attempt to modify, a BIOS setting;
- c. All records and information relating to the attachment of any peripheral to any Dominion computerized voting system, including any USB flash storage drive or other external storage media;
- d. All records and information relating to the operation of any Optical Disc Drive on any Dominion computerized voting system, including the use or attempted use of CDs or DVDs to run software;

- e. All records and information relating to any software, program, application, or code used to obtain information about the configuration, security features, contents, or vulnerabilities of any Dominion computerized voting system;
- f. All records and information relating to authorization or lack of authorization to damage or modify any Dominion computerized voting system;
- g. All records and information relating to any attempted or successful misappropriation, theft, conversion, transfer, or exfiltration of any proprietary hardware, software, or other data;
- h. All records and information relating to [REDACTED] use of another person's name, photograph, credentials, or other identifying information or documents;
- i. All records and information indicating the geographical location of any SUBJECT;
- j. All records and information indicating the state of mind of any SUBJECT, as it relates to the SUBJECT OFFENSES discussed in the Affidavit;
- k. All records and information indicating attempts by any SUBJECT to conceal an individual's involvement in the SUBJECT OFFENSES;
- l. All records and information indicating the identity of any person(s)—including records that help reveal the whereabouts of the person(s)—who communicated with any SUBJECT about any matters related to the commission of the SUBJECT OFFENSES;
- m. Evidence of who used, owned, or controlled the **LINDELL CELLPHONE** at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords,

documents, browsing history, user profiles, email, email contacts, chat, instant messaging logs, photographs, and correspondence;

- n. Evidence of software, or the lack thereof, that would allow others to control the **LINDELL CELLPHONE**, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- o. Evidence of the attachment to the **LINDELL CELLPHONE** of other storage devices or similar containers for electronic evidence;
- p. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the **LINDELL CELLPHONE**;
- q. Evidence of the times the **LINDELL CELLPHONE** was used;
- r. Passwords, encryption keys, and other access devices that may be necessary to access the **LINDELL CELLPHONE**;
- s. Volatile data and volatile memory stored in the **LINDELL CELLPHONE**;
- t. Documentation and manuals that may be necessary to access the **LINDELL CELLPHONE** or applications on the **LINDELL CELLPHONE**, or to conduct a forensic examination of the **LINDELL CELLPHONE**;
- u. Records of or information about Internet Protocol addresses used by the **LINDELL CELLPHONE**;
- v. Records of or information about the **LINDELL CELLPHONE**'s Internet activity relating to the SUBJECT OFFENSES, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the

user entered into any Internet search engine, and records of user-typed web addresses;

- w. Evidence indicating how and when the **LINDELL CELLPHONE** was accessed or used to determine the chronological context of their access, use, and events relating to the SUBJECT OFFENSES and to the user; and
- x. Contextual information necessary to understand the evidence described in this attachment.

As used above, the terms “records” and “information” include any data in any form that may be stored on any computer.

The term “computer” includes the **LINDELL CELLPHONE**.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

Executing law enforcement personnel are authorized to depress the fingerprints and/or thumbprints of Michael James Lindell onto the Touch ID or fingerprint sensor of the **LINDELL CELLPHONE**, in order to gain access to the contents of the **LINDELL CELLPHONE**. Law enforcement personnel may also hold the **LINDELL CELLPHONE** in front of the face of Michael James Lindell to activate the facial recognition feature; and/or hold the **LINDELL**

CELLPHONE in front of the face of Michael James Lindell to activate the facial recognition feature, for the purpose of unlocking the **LINDELL CELLPHONE** in order to search the contents as authorized by this warrant.

SEARCH WARRANT ADDENDUM

1. In conducting the search authorized by this warrant, the government shall make reasonable efforts to utilize search methodology that avoids searching files, documents or other electronically stored information which is not identified in the warrant.
2. If electronically stored data, information, documents or other records have been identified and seized by the government pursuant to this warrant, the government may retain the electronic storage device (e.g., computer, hard drive, mobile device, smartphone, cell phone). The person from whom the electronic storage device was seized may request that the government provide him or her with electronic copies of the data, information, documents or other records by making a written request to the United States Attorney's Office, identifying with specificity the data, information, documents or other records sought to be copied. The government must respond to all such requests within a reasonable amount of time, and must provide a copy of the electronically stored data, information, documents or other records requested unless the copies requested constitute contraband, instrumentalities, or property subject to forfeiture.
3. Nothing in this warrant shall limit or prevent the government from seizing the electronic storage device as contraband or an instrumentality of a crime or commencing forfeiture proceedings against the electronic storage device and the data contained in the device. Nothing in this warrant shall limit or prevent the owner of the electronic storage device, files, software, hardware, data, information, documents or other records from (a) filing a motion with the Court pursuant to Rule 41(g) of the Federal Rules of Criminal Procedure for the Return of Property, or (b) making a request of the government to return certain specified electronic storage devices, files, software, hardware, data, information, documents or other records.
4. The government shall establish a search methodology governing the review of seized data to ensure that no attorney-client privileged communications will be inadvertently reviewed by the prosecution team. In the event that data seized pursuant to this warrant are identified by the government as possibly containing attorney-client privileged communications, an Assistant United States Attorney, who is not a member of the prosecution team and who is not participating in the search, shall act as a "taint team" to set up an ethical wall between the evidence and the prosecution team that will prevent any privileged material from getting through to the prosecution team.