EXHIBIT 1

UNITED STATES DISTRICT COURT

FILED IN THE
UNITED STATES DISTRICT COURT
DISTRICT OF HAWAII
May 14, 2025 4:28 PM
Lucy H.Carrillo, Clerk of Court

~~SEALED~~

BY ORDER OF THE COURT

for the

District of Hawaii

NOTICE: Pursuant to LR79.2 Any Search Warrant Return will be unsealed one (1) year after the file date of this search warrant application

In the Matter of the Search of

(Briefly describe the property to be searched or identify the person by name and address)

INFORMATION ASSOCIATED WITH THE SNAPCHAT ACCOUNT "COW_KNEES" THAT IS STORED AT PREMISES CONTROLLED BY SNAP INC.

Case No. MJ25-364-RT

FILED UNDER SEAL PURSUANT TO CRIMLR5.2(a)(1)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, 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 *(identify the person or describe the property to be searched and give its location):*

See Attachment A.

located in the Central District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

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 Section	*Offense Description*
18 U.S.C. §§ 371, 1951, 2251, 2252A, 2261A, 1512	Conspiracy; Extortion; Production of Child Pornography; Distribution, Receipt, and Possession of Child Pornography; Cyberstalking; Obstruction of Justice

The application is based on these facts:

See attached Affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Kyle Charles Rawlinson, FBI SA

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by Telephonic Communication *(specify reliable electronic means).*

Date: May 14, 2025

City and state: Honolulu, Hawaii

Wes Reber Porter
United States Magistrate Judge

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF HAWAII

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH THE SNAPCHAT ACCOUNT "COW_KNEES" THAT IS STORED AT PREMISES CONTROLLED BY SNAP INC.	MJ25-364 RT **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Kyle Rawlinson, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain Snapchat account—"cow_knees" (the "ACCOUNT")—that is stored at premises owned, maintained, controlled, or operated by Snap Inc. ("Snap"), an electronic communications service and/or remote computing service provider headquartered in Santa Monica, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Snap to disclose to the government copies of the information (including the content

of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been since April 2022. I am currently assigned to the Honolulu Division's Joint Terrorism Task Force. My responsibilities include, but are not limited to, the investigation of domestic and international terrorism. I have experience conducting investigations related to counterintelligence, counterterrorism, child pornography, child abuse, narcotics, and fraud. I have investigated criminal violations relating to child exploitation and child pornography, including violations pertaining to the illegal production, distribution, receipt, and possession of child pornography. During such investigations and by consulting with other law enforcement agents on the same, I gained experience identifying distinguishing features of children at various stages of growth based on anatomical development and developmental cues that aid in accurately determining the ages of minors depicted in visual media. In support of my investigations, I have utilized court authorized search warrants and subpoenas; conducted physical surveillance; handled confidential informants; and interviewed subjects and witnesses. Due to my training and experience as a Special Agent, I am familiar

with the United States Criminal Code. In past criminal investigations, I executed search warrants, resulting in valuable physical and digital evidence collection, seized assets, and subjects agreeing to cooperate with the government.

3. The facts in this affidavit come from my observations, my training and experience, and information obtained from other law enforcement agents. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter. Throughout this affidavit, I use square brackets "[ ]" to anonymize personal identifiers and investigation-sensitive usernames.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that the following violations have been committed by Rumaldo Valdez ("Valdez") and other persons: 18 U.S.C. §§ 371 (Conspiracy), 1951 (Extortion), 2251 (Production of Child Pornography), 2252A (Distribution, Receipt, and Possession of Child Pornography), 2261A (Cyberstalking), and 1512 (Obstruction of Justice). There is also probable cause to search the information described in Attachment A—the ACCOUNT—for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

Discord Server (the "Offending Server")

6. In 2021, law enforcement began investigating a particular Discord server (hereinafter, the "Offending Server"). The Offending Server is linked to members of a group loosely identified with an ideological extremist group (hereinafter, "Extreme Group"). In 2021, law enforcement received CyberTips from Discord concerning the Offending Server and Extreme Group. As detailed below, the CyberTips reported that members of Extreme Group were involved in producing and sharing child pornography using Discord, including via the Offending Server, and were extorting minors into creating self-harm material and child pornography and then uploading that content to Discord.

7. As a result of these CyberTips, the FBI began investigating several Discord accounts linked to the Offending Server and Extreme Group, including variants of the username "Duck" (e.g., "Duck.#8030") and "M[username]."

First CyberTip

8. On January 17, 2021, Discord submitted a first CyberTip to NCMEC. In that CyberTip, NCMEC reported that, on January 17, 2021, someone using the Discord account "Duck.#8030" uploaded a file containing child pornography to Discord. According to the NCMEC report, employees of Discord viewed the file and determined it was likely child pornography. NCMEC reported that, per Discord, the Discord account "Duck.#8030" was linked to the verified[1] email address "boobuh[number]@gmail.com" and the user, at the time of the upload, was using an IP address ending in -178.28. The uploaded file was an image file ("image0.jpg"). That file is an image of a white male, approximately twelve years old. The male is looking at the camera, wearing headphones, and his penis is erect. The male is in a bathroom, leaning back across the wall with a blue shower curtain. He is wearing a sweater but does not appear to be wearing any pants. The focal point of the image is the male's erect penis. The age of the male is estimated based on his size, facial structure, and physical development, which includes minimal pubic hair and undescended testes. Based on my training and experience, I believe this material depicts a minor engaged in sexually explicit conduct as defined under

[1] Verified means that Discord sent an email to the email address and the user of that email address responded to that email, thereby "verifying" the email address was used by the Discord account owner.

18 U.S.C. § 2256(2)(A)(v) ("lascivious exhibition of the anus, genitals, or pubic area of any person") and therefore is "child pornography" as defined under 18 U.S.C. § 2256(8).

Second CyberTip

9. On January 23, 2021, Discord submitted a second CyberTip to NCMEC. In that CyberTip, NCMEC reported that, on January 23, 2021, someone using the Discord account "Duck.#8030" uploaded two files containing child pornography to Discord. According to the NCMEC report, employees of Discord viewed both files and determined they were likely child pornography. NCMEC reported that the "Duck.#8030" account was linked to the verified email address "boobuh[number]@gmail.com" and the user, at the time of the uploads, was using the IP address ending in -178.28. One of the files uploaded was an image file ("62z2vgy6.jpg"). That image file depicts a prepubescent white female, approximately eight to ten years old, who is smiling at the camera while using her hand to spread her vagina open and also exposing her open anus to the camera. I estimate the age of the female based on her size, facial structure, and lack of physical development. The female is wearing a floral shirt and headband but does not appear to be wearing any pants. The focal point of the image is the female's open vagina and open anus. Based on my training and experience, I believe this material depicts a minor engaged in sexually explicit conduct as defined under 18

U.S.C. § 2256(2)(A)(v) ("lascivious exhibition of the anus, genitals, or pubic area of any person") and therefore is "child pornography" as defined under 18 U.S.C. § 2256(8).

Third CyberTip

10. On February 11, 2021, Discord submitted a third CyberTip to NCMEC. In that CyberTip, NCMEC reported that, on February 11, 2021, someone using the Discord account "Duck..#8030"[2] uploaded a file containing child pornography to Discord. According to the NCMEC report, employees of Discord viewed the file and determined it was likely child pornography. NCMEC reported that, per Discord, the Discord account "Duck..#8030" was linked to the verified email address "retardsunite@[domain].net" and the user, at the time of the uploads, was using the IP address ending in -178.28. The uploaded file was a graphic image file ("002.gif"). That image is an animated image file depicting a white female, appearing to be less than ten years old, and who has an adult male's erect penis interested into her mouth. The adult male is placing his hand on the

[2] This is a slight variant of the Discord account linked to the Second CyberTip ("Duck.#8030") because it contains an extra period between "Duck" and the "#" sign. Based on my training and experience, it is common for users of Discord (and other social media platforms), particularly after being banned for engaging in prohibited activities on the platform, to create new accounts using slightly different variants of their original account name. This is done so that other users can recognize the account owner remains the same person.

back of the female's head, forcing his entire penis into her mouth, and causing her to gag and push him away. I estimate the age of the female based on her size, facial structure, and lack of physical development. Based on my training and experience, I believe this material depicts a minor engaged in sexually explicit conduct as defined under 18 U.S.C. § 2256(2)(A)(i) ("sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal") and therefore is "child pornography" as defined under 18 U.S.C. § 2256(8).

Fourth CyberTip

11. On February 27, 2021, Discord submitted a fourth CyberTip to NCMEC. In that CyberTip, NCMEC reported that, on February 3, 2021, someone using the Discord account "m[username]" was involved with the Extreme Group and was extorting minor females into creating self-harm material and child pornography and then uploading images and videos of that activity to Discord. According to the NCMEC report, employees of Discord viewed numerous files and chat logs related to the Discord account "m[username]" and determined the activity was criminal in nature. For example, Discord uploaded a video file ("Daddy_Walks_In.mp4"), which I have viewed, depicting a screen recording of a Discord chat. During the chat, the user of Discord account "m[username]" can be heard coercing a minor into committing acts on camera, and then threatening the minor's guardian after the guardian enters the scene. During the exchange, the

user of Discord account "m[username]" claimed to have seen the minor naked and knew the minor was only 16 years old. The NCMEC report also contained numerous files uploaded by Discord account "m[username]" and viewed by Discord employees, which I also viewed. They include:

- an image file ("m[name]slave10.jpg") depicting a female child with a black eye holding up a sign stating, "M[username] has me and my 2 year old sister captive. He's a sick man."
- an image file ("m[-]slave2.png") depicting a clothed prepubescent child holding up a sign stating, "M[username]."
- a video file ("[Extreme Group].mp4") depicting a video of numerous clothed, prepubescent females.
- numerous text files containing chat records between Discord account "m[username]" and a deleted Discord account ("Deleted User 6cf779ba") which, based on cross-referenced information from Discord, represents Discord account "Duck.#8030" after it was deleted.

12. One of the chat logs contains communications between Discord account "m[username]" and Discord account "Duck.#8030" on January 13, 2021, captured below:

m[username]	extorted a 12 year old ATTACHMENT: "unknown.png" [Affiant's note: this image file is a self-portrait of a female in a white bra and yellow underwear, who appears, based on my training and experience investigating child sex offenses, to be between the ages of ten and fourteen given her lack of physical development, facial structure, and overall body size. I

	believe this image are the same minor female that "Duck.#8030" and "m[username]" discuss having extorted in the chat below.]
Duck.#8030	looks like that dudes sister
m[username]	it is
Duck.#8030	wait what
Duck.#8030	How
m[username]	I said if she sent me lewds on snap i would unlock her brothers pc
m[username]	she sent me lewds and i sc'ed [Affiant note: "sc'ed" = "screenshotted"]
Duck.#8030	LOL
m[username]	blackmailed her
m[username]	made her go on cam
Duck.#8030	AHAAHAHAH
Duck.#8030	she's never forgetting this
m[username]	she was crying
Duck.#8030	it will forever be a memory of "when i was 12"
Duck.#8030	scary internet man did things to me
m[username]	I told her that I was 27
Duck.#8030	did brother know?
m[username]	Yeah
Duck.#8030	how'd it end
Duck.#8030	like how'd you finish the gc [Affiant note: "gc" = "group chat"]
m[username]	i told her that i would fuck up her life
Duck.#8030	yeah my sleep schedule was fucked i went to bed after the tranny
m[username]	ATTACHMENT: "unknown.png" [Affiant's note: this image file is another self-portrait of a female in a white bra and yellow underwear, who appears, based on my training and experience investigating child sex offenses, to be between the ages of ten and fourteen given her lack of physical development, facial structure, and overall body size. I believe this image are the same minor female that

	"Duck.#8030" and "m[username]" discuss having extorted.]
Duck.#8030	AHAHAHAHHA
Duck.#8030	wtf is THAT
m[username]	kinky middle schooler
Duck.#8030	only with you could i wake up at 7am and see some 12 year old sexy pics
m[username]	yeah i had a pedo moment
m[username]	Sucks
Duck.#8030	old m[name] came out

2021 Federal Search Warrant

13. In 2021, pursuant to federal search warrant, law enforcement obtained a video depicting users of the Offending Server interacting with a minor female. The video shows members of the Offending Server telling the minor female to "go get scissors." When the minor female hesitates, one of the participants threatens her: "I'm talking more about the social part of it having all of your family seeing your naked body, maybe your friends? You go to school right? You know we don't care about anything right? You can say it's illegal, we don't care, we don't care about you, so you should listen to what we're saying." The minor female, who is crying, then retrieves the scissors, and the Offending Server users tell the minor female to cut her hair, with one user declaring, "It's chopping time!" The minor female cries as she cuts her hair, and one of the members tells her to "shove" her cut ponytail up her vagina.

Extreme Group Compilation Video

14. The fourth CyberTip also contained a video file, uploaded by "m[username]" on February 3, 2021, entitled "[Extreme Group].mp4." According to the NCMEC report, employees of Discord viewed this video and determined it contained evidence of criminal activity. The video is approximately one minute long and begins with a male (presumptively, the token figurehead for Extreme Group) recording himself sitting at his computer. The words Extreme Group are overlaid in red font, followed by the caption "Discord.gg/[Extreme Group]" (which is the URL to join the Offending Server). As the video progresses, several minor females are depicted recording themselves while repeating the phrase, "hail [Extreme Group]." The final 40 seconds of the video is a portion of the hair-cutting video described above, and the video ends by quickly flashing between satanic imagery and pictures of the same male (i.e., the token figurehead) seen in the beginning of the video. The video is the same "[Extreme Group].mp4" file obtained from Discord in connection with the fourth CyberTip.

15. In 2023, a minor female spoke to law enforcement. She said she was familiar with the users of the Offending Server. She described the primary members as "M[username]," "Duck," "H[username]," "O[username]," and "F[username]." She reported that members of the Offending Server extort female

victims into providing nude images or videos and performing self-harm, including cutting body parts with a razor.

CHS Information Concerning the Offending Server and "Duck.#8030"

16. In early 2024, an FBI confidential human source ("CHS") with direct knowledge of the activities of the Offending Server provided information to law enforcement. The CHS has pled guilty to multiple federal felony convictions for receiving child pornography and cyberstalking related to the CHS's involvement with, among other things, the Offending Server. In connection with those felony convictions, the CHS admitted that the CHS, working with other members of the Offending Server, used Discord to threaten and coerce minors into creating child pornography and self-harm material, and that the CHS received child pornography as a result of those efforts.

17. In 2024, the CHS—who, at the time, was seeking leniency from the government in connection with sentencing—provided information about illegal activities on the Offending Server and Extreme Group. The CHS admitted to being an active participant on the Offending Server and involved with other participants to extort minors into creating and sending self-harm material and child pornography, install malicious software on victims' computers, "swatting," and sharing child pornography and other graphic images while "Zoom Bombing." The CHS identified "Duck" as an active member of the Offending Server, and said the

CHS understood "Duck" was from somewhere near Oceanside, California,[3] interested in coding and computer science, and was in high school when they were interacting with one another. The CHS said that "Duck" sent victims links to malicious files and used malware for the purpose of extorting victims. The CHS stated that members of the Offending Server, including "Duck," downloaded and shared child pornography and self-harm materials.

18. CHS also said that "Duck" was skilled at editing videos and created some of the media used to promote the Offending Server and Extreme Group, including creating video montages of their activities. The CHS stated "Duck" shared this material on other Discord servers for shock value. The CHS said that "Duck" edited the "hair cutting" video described above, which included the full name of the minor victim, and stated that, in the CHS's opinion, "Duck" had to download the recorded content to "Duck's" computer to edit the videos.

19. The CHS also reported having witnessed "Duck" record online extortions. For example, the CHS reported that, on one occasion, the CHS witnessed "Duck" coerce a minor female (approximately fourteen to sixteen years old) into creating a video showing the minor female masturbating. "Duck" then

[3] The CHS reported that "Duck" used a virtual private network to obscure his identity, but that, on some occasions, "Duck" forgot to use a virtual private network, and the CHS identified the IP address used by "Duck" as originating from Oceanside, California.

later used that video to coerce the minor female into cutting the word "Duck" into her arm. The CHS reported that the minor female, while crying, recorded herself cutting the name "Duck" into her arm, provided that recording to "Duck," and that "Duck" then saved and posted that material (i.e., a "fan sign") online, including on Discord. The CHS reported that "Duck" also made a video clip of the material and identified the minor female by name in the video clip, which "Duck" promoted online.

Valdez's Connection to "Duck.#8030"

20. Subscriber information for the IP address ending in -178.28 for the time periods associated with the first, second, and third CyberTips (described above) returned the following information:

- Subscriber Name: Rumaldo Valdez
- Service Address: [street number] Cayucos Way, San Diego, CA, 92129
- Billing Address: [street number] Old West Ave., San Diego, CA 92129
- Phone Number: [Southern California number] -5304

21. In 2023, investigators obtained subscriber information for the email address "boobuh[number]@gmail.com" (linked to the Discord account "Duck.#8030") from August 2022 through May 2023:

- Potential Name: Rumaldo Valdez
- Several IP addresses located in Pensacola, Florida

- Phone Number: [Southern California number] -5304
- Recovery Phone Number: [Southern California number] -0114

22. Subsequent investigative activity and military database checks revealed that Valdez enlisted in the Navy on June 22, 2021, began training at Great Lakes, Illinois, in December 2021, completed training in Pensacola, Florida between June and August 2022, and was permanently assigned to NCTAMS, Wahiawa, Hawaii beginning August 24, 2023. Military records list Valdez's phone number as [Southern California number] -0114 (i.e., the "Recovery Phone Number" linked to "boobuh[number]@gmail.com," which is the email address linked to Discord account "Duck.#8030"). Military records list Valdez's "Home of Record" as [street number] Old West Ave., San Diego, CA 92129 (i.e., the "Billing Address" for the IP address ending in -178.28, which was used to upload the child pornography described above in the first three CyberTips).

23. In March 2024, investigative agents obtained the computer-user profile for Valdez from the Navy's government-owned server. The profile contains, among other things, internet activity. Navy members, like Valdez, are notified that they do not have a privacy interest in internet activity when using Navy computers and networks because they are government property and are subject to monitoring to ensure compliance with security protocols and regulations. A review of the internet activity for Valdez's profile between October 2023 and February 2024 revealed that,

while using a Navy computer and network, and his Navy-issued computer-user profile, Valdez accessed:

- approximately 10,000 Discord chat URLs (indicative of frequent access to the Discord platform)
- an image of a human foot with the word "Duck" written on the toes;
- an image of a small child bound and gagged with tape;
- multiple logins for "boobuh[number]@gmail.com";
- the monikers "H[username]" and "O[username]" (both associated with the Offending Server and Extreme Group); and
- numerous internet searches related to hacking, remote access tools, malware, including commands to remove all files and directories, and delete a registry through a single command.

24. On March 30, 2024, investigators obtained subscriber information for the email address "boobuh[number]@gmail.com" (and linked to the Discord account "Duck.#8030") from March 2024:

- Account Name: Duckyy
- Display Name: shrimp valdez
- Several IP addresses located in Oahu, Hawaii
- Recovery Phone Number: [Southern California Number] -0114

25. On May 30, 2024, the Honorable Kenneth J. Mansfield, United States Magistrate Judge for the District of Hawaii, issued a federal search warrant authorizing the search of Valdez's person, residence, and vehicle for, among other

things, computers or storage media used as a means to commit the federal offenses of conspiracy, extortion, production of child pornography, cyberstalking, and distribution, receipt, and possession of child pornography.

26. On May 31, 2024, investigators executed the search warrant on Valdez and his residence located at Naval Computer and Telecommunications Area Master Station Pacific, a United States military installation in Wahiawa, Hawaii. The search resulted in the seizure of an operating-system drive housed within a desktop-computer tower located on Valdez's desk (hereinafter, the "OS drive"), a SanDisk solid state drive located on the same desk (hereinafter, the "SanDisk SSD"), a Maxtor solid state drive extracted from the desktop-computer tower (hereinafter, the "Maxtor SSD"), and an iPhone 14 located on Valdez's person. While examining the Maxtor SSD, investigators found the "boobuh[number]@gmail.com" email address stored as Windows user profile data. Investigators found another email address, "duckk@[domain].net," stored as Windows user profile data. The "duckk@[domain].net" email address was associated with an additional child pornography CyberTip against Discord user "Duck#8030," not summarized above. While examining the SanDisk SSD, investigators encountered a virtually encrypted container titled, "M.2 Container." And while examining the OS drive, investigators found a text file saved under

Windows user account "17604" titled, "illegal chars.txt." Investigators used a 20-character string inside that text file to unlock, i.e., decrypt, the "M.2 Container."

27. On the Maxtor SSD, investigators found approximately 19 thumbnail-cache files containing child pornography and depicting minor(s) engaged in sexually explicit conduct. As one example, an image file contains a screenshot of a direct-message chat between Discord user "S[username]" and another Discord user. Displayed within that chat is a picture of a minor female, approximately 8 to 12 years old, wearing a butterfly necklace and surrounded by 7 erect, adult penises. The minor female's face is at waist level with the surrounding males, and her arm is outstretched, flicking off the camera. Her mouth is open, and her face is covered in what appears to be semen. At least some of the surrounding males appear to be masturbating. As a second example, an image file contains a screenshot of Discord server chat between various Discord users, e.g., "E[username]" and "M[username]." "E[username]" is sharing a picture of the following with other chat members: A minor female, approximately 6 to 7 years old, performs fellatio on an adult male with tattoos on his left arm. The adult male is forcefully inserting his penis into the minor female's mouth, with the adult's hand grabbing the back of the minor's head.

28. On the SanDisk SSD, within the "M.2 Container," investigators found approximately 4 image files and 20 video files containing child pornography and

depicting minor(s) engaged in sexually explicit conduct. As one example, an image file contains three pictures joined horizontally in a timeline-type format. All three depict a female infant, approximately 1 to 2 years of age, with curly black hair and an erect, adult penis. In the leftward picture, the female infant is lying on her back while the adult grasps his erect penis above the infant's vagina. In the middle picture, the penis penetrates the infant's vagina. And in the rightward picture, the infant is pushing up from her back, appearing to have semen on her lower abdomen and appearing to have a red and swollen vagina. As a second example, a video file shows a recorded chat session on the Offending Server between "Duck," "M[username]," and others. The recording begins by displaying a picture of a deceased infant with his/her neck slit open. During the initial third of the video, "M[username]" appears to hack into the Discord account of "S[username]." In the middle third of the video, "M[username]" displays for the chat participants a log of direct messages between "M[username]" and "Duck#8030." The log shows "Duck" having uploaded and messaged to "M[username]" the same child-pornography image described first in paragraph 27, above, among others. "M[username]" then posts that image into a different Discord server, using the hacked "S[username]" account. In the last third of the video, the server members discuss "Duck" and child pornography: "M[username]" says, "Nah, Duck just supplies me like instantly. Need cp, boom, instantly. I get a

bunch of cp." Another user interjects, "[Duck,] you probably [sic] watch it on your free time." "Duck" replies, "oh yeah, I do it all the time. I get bored. Normal porn won't do it for me anymore."

29. Further, on the "M.2 Container," investigators found a video file containing a screen recording of Discord user "Duck." participating in the "e-rape" channel on a notorious Discord server. In the approximately 25-minute-long recording, the Discord user "Cl[username]" live streams multiple videos of the torture of a female toddler. In each video, the toddler is naked, crying in distress, and appears to be between the ages of 2 to 4 years old. The first streamed video starts by showing an age-difficult female twisting and pinching the toddler's nipples while the toddler screams in pain. The female then slaps the toddler's vagina repeatedly with her hands. Next, the female sits the toddler up and places the toddler's hand in the female's vagina. While doing so, the female kicks the toddler in the head, keeping the toddler's hand in the female's vagina during the assault. The female then removes the toddler's hand from the female's vagina and places it into the toddler's mouth, repeatedly. To end the first video, the female lays the toddler on the toddler's back and forcibly opens the toddler's vagina, which causes the toddler to, again, scream in pain. "Cl[username]" then live streams a second video of what appears to be the same toddler and age-difficult female: The female forces an ice cube into the toddler's anus and vagina, after

which the female rubs the ice cube over the toddler's body. The female then tapes the toddler's mouth shut and the toddler's feet to a bar, leaving the toddler hanging upside down. The female places clips on the toddler's nipples while the toddler is gagged and hanging upside down, and the female repeatedly slaps the toddler's vagina. Next, the female forcibly opens the toddler's vagina and places a clip on what appears to be the toddler's vagina. The female then binds the toddler's hands to the same bar as the toddler's feet and rubs ice over the toddler's body. While the toddler is hanging by her feet, the female begins burning the toddler with what appears to be either a match or a candle. The toddler struggles and thrashes about while being burned. "Cl[username]" live streams a third video of what appears to be the same toddler and age-difficult female. The third video begins by showing the toddler hanging upside down over a toilet while the female urinates in the toddler's mouth. Next, the female hangs the toddler upside down over a mattress and tapes the toddler's mouth shut and hands behind the toddler's back. The female then slaps the toddler across the face and begins inserting unknown objects into the toddler's vagina, leaving those objects inserted while the toddler hangs upside down, still bound and gagged. While the toddler is hanging, the female hits the toddler with a belt and burns the toddler repeatedly on various parts of the toddler's body with what appears to be either a match or candle.

30. Also on the SanDisk SSD, within the "M.2 Container," investigators found a video file of a screen recording created on May 2, 2021 in which the computer operator accesses the "illegal chars.txt" file on the desktop for the "17604" Windows user, copies the same 20-charater string mentioned in paragraph 7, above, and uses that string as a password to virtually decrypt the "A:\M.2 Container," in order to access a "fansigns" folder. During one portion of the video, a Discord chat window and display name "Duck v7" are visible. During another portion of the video, the computer operator navigates through files on the "M.2 Container" using a file explorer, and the filename "james fansign" is displayed alongside a preview icon for that image file. The preview icon shows what appears to be a pre-pubescent boy holding a "Duck#8030" fan sign, with his genitalia exposed in a lewd and lascivious pose.

31. The last access date of the "M.2 Container" on the SanDisk SSD is September 26, 2023. Valdez moved to Hawaii around August 2023. Following the May 31, 2024 search operation, investigators located the "james fansign" image file on the "M.2 Container," within the SanDisk SSD. That image file's contents match the preview icon described two paragraphs above.

32. On the iPhone 14, investigators found a Snapchat message between user "cow_knees" and "Cd[username]," wherein "cow_knees" provides his alternative Discord account, "Duck v7#8030," because he was previously banned

on Discord. The "cow_knees" side of the conversation corresponds to the side assigned to the iPhone operator and is referenced as "cow_knees Duck (owner)" in the Snapchat application on the iPhone.

33. Also while searching the iPhone 14, investigators discovered the following two conversations on the iPhone's Snapchat application:

Chat #1

f[username] 12/31/2020 10:56:49 AM(UTC+0)	i didn't see what the hell you sent
f[username] 12/31/2020 10:57:02 AM(UTC+0)	let it load asshole
f[username] 12/31/2020 10:57:09 AM(UTC+0)	my wifi is ass rn
cow_knees Duck (owner) 12/31/2020 10:57:17 AM(UTC+0)	you may never know then
f[username] 12/31/2020 10:57:26 AM(UTC+0)	no that's not fair
cow_knees Duck (owner)	it's child porn

12/31/2020 10:57:33 AM(UTC+0)	
f[username] 12/31/2020 10:57:43 AM(UTC+0)	Why
cow_knees Duck (owner) 12/31/2020 10:57:48 AM(UTC+0)	it's a small child
cow_knees Duck (owner) 12/31/2020 10:57:52 AM(UTC+0)	holding a piece of paper
f[username] 12/31/2020 10:57:57 AM(UTC+0)	idk to believe that or not
cow_knees Duck (owner) 12/31/2020 10:58:06 AM(UTC+0)	do you think i'd lie about that

23. On November 19, 2024, investigators issued a data preservation request to Snap for the ACCOUNT.

24. Around June 19, 2024—before the preservation request and after the search warrant operation on May 31, 2024—investigators received notice of seven failed login attempts on the ACCOUNT from an Android device with an IP address geolocating to Mililani, Hawaii. In my training and experience, I assess

that Valdez was likely attempting to access the ACCOUNT from a phone other than his iPhone 14, which had been seized during the May 31, 2024 search warrant operation. Valdez likely had the ACCOUNT's access information tied to his iPhone 14, thus preventing two-factor authentication, resulting in the failed login attempts. In my training and experience, I also know that users of online services like Snap can reset account-access information, e.g., devices providing two-factor authentication, through various security protocols defined by services providers. If Valdez successful reset the ACCOUNT's access information, he may have gained access to the ACCOUNT after the failed login attempts, but before the November 19, 2024 data preservation request, potentially providing him a window in which he could have tampered with or deleted data relevant to this investigation.

BACKGROUND CONCERNING SNAP[4]

25. Snapchat is headquartered in Santa Monica, California, and owns and operates a free access social networking website of the same name that can be accessed at http://www.snapchat.com. Snapchat is an application for sending and receiving self-destructing-type messages, pictures, and videos.

[4] The information in this section is based on information published by Snap on its website, including, but not limited to, the following webpage: "Snap Inc. Law Enforcement Guide," https://storage.googleapis.com/snap-inc/privacy/lawenforcement.pdf.

26. A "Snap" is a picture or video message taken and shared with other Snapchat users in real-time. The sender of a snap has the option of setting a timer for how long a snap can be viewed. Once a snap has been viewed it is deleted from the company's system and is no longer visible to the recipient. Snapchat users can send text messages to others using the Chat feature. Once a user leaved the Chat screen, messages viewed by both the sender and the receiver will no longer be visible. The application notifies other users when they are online so they can begin messaging each other. In addition, Snapchat users can send pictures to other users by utilizing the camera on their device. Pictures can also be sent from the saved pictures in the photo gallery of the device. Accessing a Snapchat account and "snaps" constitute "electronic communications" within the meaning of 18 U.S.C. § 3123. *See* 18 U.S.C. §§ 3127(1) and 2510(12).

27. "Stories" are a collection of user-submitted "Snaps" from different locations and events. A Snapchat user, with the location services of their device turned on, can contribute to a collection of snaps regarding the event. For example, multiple different Snapchat users at a rave could all contribute to the same "Our Stories" collection by sharing their snaps, even if they do not know each other. Users can also view "Our Stories" events if they are not actually present at the event by subscribing to the story. In addition to "Our Stories", a Snapchat user can keep a sort of photo/video diary using the "Story" feature. Each snap in a "Story"

documents the user's experience. Users can manage their privacy settings so that their Story can be viewed by all Snapchatters, their friends, or a custom audience. A user can also submit their Snaps to our crowd-sourced service "Our Story", which enables their Snaps to be viewed by all Snapchatters in Search and Snap Map. Snap's servers are designed to automatically delete a Snap in a user's Story 24 hours after the user posts the Snap, but the user may delete part or all of the Story earlier. Submissions to Our Story may be saved for longer periods of time.

28. "Memories" is Snapchat's cloud-storage service. Users can save their sent or unsent Snaps, posted Stories, and photos and videos from their phone's photo gallery in Memories. Content saved in Memories is backed up by Snap and may remain in Memories until deleted by the user. Users may encrypt their content in Memories (called "My Eyes Only"), in which case the content is not accessible to Snap and cannot be decrypted by Snap.

29. While a Snapchat message may disappear, the record of who sent it and when still exists. Snapchat records and retains information that is roughly analogous to the call detail records maintained by telecommunications companies. once a Snap has been opened by all recipients, the content is permanently deleted and unavailable. If a Snap is unopened by one or more recipients, it may remain on Snap's servers for up to 30 days. A Snap that has been posted to a user's Story can be viewed for up to 24 hours. Typically, the posted Snap is permanently deleted

and unavailable 24 hours after being posted to the user's Story. Chat content will typically only be available if the sender or recipient has chosen to save the Chat.

30. This includes the date, time, sender, and recipient of a snap. Additionally, Snapchat stores the number of messages exchanged, which users they communicate with the most, message status including if and when the message was opened, and whether the receiver used the native screen capture function of their device to take a picture of the snap before it disappeared. A user can type messages, send Snaps, audio notes, and video notes to friends within the Snapchat app using the Chat feature. Our servers are designed to automatically delete one-to-one chats once the recipient has opened the message and both the sender and recipient have left the chat screen, depending on the user's chat settings. Snap's servers are designed to automatically delete unopened one-to-one chats in 30 days. Users can also chat in groups. Chats sent in groups are deleted after 24 hours whether they are opened or not. A user can save a message in Chat by pressing and holding the message. The user can unsave the message by pressing and holding it again. This will delete it from our servers. Users can also delete chats that they have sent to a recipient before the recipient has opened the chat or after the recipient has saved the chat.

31. If a user has device-level location services turned on and has opted into location services on Snapchat, Snap will collect location data at various points

during the user's use of Snapchat, and retention periods for location data vary depending on the purpose of the collection. Users have some control over the deletion of their location data in the app settings.

32. Snapchat users can search for friends, groups of friends, and find new friends to add. Users can also search their own Memories to find prior Snaps. Snapchat stores a user's search terms, approximate location, and the time the search was conducted.

33. Snapchat asks users to provide basic contact and personal identifying information to include date of birth. When a user creates an account they make a unique Snapchat username. This is the name visible to other Snapchat users. An email address is required to register a Snapchat account and a new user must also provide a mobile phone number. This phone number is verified during the registration process. Snapchat sends an activation code which must be entered before proceeding with the registration step. However, a user may elect to bypass entering a phone number so one may not always be present in the user's account. Snapchat also retains the account creation date.

34. Snapchat stores device information such as the model, operating system, operating system version, mobile device phone number, and mobile network information of devices used in conjunction with the service. They also collect unique device identifiers such as the Media Access Control address and the

International Mobile Equipment Identifier or Mobile Equipment Identifier of devices used to access Snapchat. In the event the Snapchat user's application crashes, the company also collects a list of other installed applications on the device to detect any potential software conflicts.

35. Snapchat has a "Group Stories" feature allowing multiple users to contribute photos and videos to the same "Story," a collection of posts that stay viewable for a limited amount of times. Snapchatters can name their group story and invite other users and "friends" by username to add content. The group Stories will disappear if 24 hours pass without a user adding a new photo or video.

36. In some cases, application account users will communicate directly with the service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Application providers typically retain records about such communications, including records of contacts between the user and the providers support services, as well as records of any actions taken by the provider or user as a result of the communications. In addition, application providers often have records of the IP addresses used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help identify which computers or other devices were used to access the account.

37. Snap maintains logs containing metadata about a user's Snaps, Stories, Chats. This can further include account change history: a log of changes to the account made by the user, including dates/times of changes in registration email address or phone number, birthdate, and display name. Even further, this can include history on basic information about Snaps the user has recently sent and received, including the sender, recipient, type of Snap, and date.

38. In my training and experience, evidence of who was using an application account may be found in address books, contact or buddy lists, email addresses in the account, and attachments to electronic messages, including pictures and files.

PROBABLE CAUSE FOR SPECIFIED SNAP ACCOUNT SERVICES

23. In addition to basic subscriber information, the following information is sought for the Snap ACCOUNT: chat content; associated accounts; device information; Friends; history and logs containing metadata about Snaps, Stories, Chats; location data; Memories content; encrypted My Eyes Only content; search history; and "Our Story" and crowd-sourced content.

24. There is probable cause to believe that the ACCOUNT's Chat content will contain fruits, contraband, evidence, and/or instrumentalities of the specified offenses because the user behind the "cow_knees" Snapchat account, believed to be Valdez, has already exchanged child pornography over Chats, as explained

above. Also, Valdez ("cow_knees") has transferred a co-conspirator ("Cd[username]") from one of his Discord accounts to another, using a Chat in Snapchat. Further, in a chat detailed above, "Duck.#8030" and "m[username]" mention a victim sending "lewds on snap"—there is thus probable cause that the ACCOUNT's Chat content will contain direct evidence of distribution, receipt, and possession of child pornography, as well as extortion and cyberstalking.

25. There is probable cause to believe that the ACCOUNT's associated Snapchat accounts will contain fruits, contraband, evidence, and/or instrumentalities of the specified offenses because the user behind the "cow_knees" Snapchat account, believed to be Valdez, has been linked to various criminal activities, including the distribution, receipt, and possession of child pornography, as well as extortion and cyberstalking. Evidence collected from other platforms, such as Discord, indicates that Valdez used various online identities to communicate with minors and coerce them into producing child pornography and self-harm materials. Further, investigative findings show that "cow_knees" was used for communications related to the sharing of child pornography and communicating with co-conspirators. The link between the Snapchat account and other devices and accounts associated with Valdez, such as his military-issued computer and email addresses tied to his Discord activities, strengthens the belief that the Snapchat account will contain additional evidence

relevant to these offenses. Moreover, the metadata and the interactions on the Snapchat ACCOUNT, especially those related to exchanging explicit content, are consistent with patterns of behavior typically seen in individuals who maintain and distribute illegal pornography. The presence of these communications and images on a widely used and secure platform like Snapchat further suggests the related account will yield crucial evidence related to Valdez's involvement in child exploitation and online extortion activities.

26. There is probable cause to believe that the ACCOUNT's device information will contain fruits, contraband, evidence, and/or instrumentalities of the specified offenses because investigative findings show that the device associated with the "cow_knees" Snapchat has been used to exchange child pornography and to facilitate communications that coerce minors into producing self-harm materials, consistent with patterns of sexual extortion and exploitation. Data recovered from other devices belonging to Valdez, such as his military-issued computer, have shown extensive interactions with encrypted containers and malware, all pointing to the likelihood that the devices associated with the "cow_knees" ACCOUNT will hold similar incriminating evidence. If identified and located by investigators, these additional devices' storage is expected to contain relevant communications, media files, and metadata that could help establish the Valdez's intent and involvement in these criminal offenses. Further,

the other-apps-installed data collected by Snap during application crashes may permit investigators to piece together Valdez's digital techniques, tactics, and procedures, including other applications he may be using to hide, encrypt, or distribute child pornography.

27. There is probable cause to believe that the ACCOUNT's Snapchat Friends will constitute fruits, contraband, evidence, and/or instrumentalities of the specified offenses because individuals in the "cow_knees" account's contact list are likely to be involved in or have knowledge of the illicit activities tied to the production, distribution, and possession of child pornography, as well as sexual extortion and cyberstalking. Investigative findings from other platforms, including Discord, suggest that the individuals associated with the "Duck" account, which is closely linked to Valdez and "cow_knees," have been engaged in these criminal activities, including the coercion of minors into producing explicit material. Thus, it is reasonable to believe that the Snapchat Friends list may include individuals who were either directly involved in or served as recipients of illicit content, or who participated in the discussions and exchanges that facilitated these crimes. The social connections on this platform could provide further evidence of the network of individuals involved in the exploitation of minors, and examining the Snapchat Friends could uncover additional perpetrators, witnesses, or evidence of the ongoing distribution and possession of child pornography. Unveiling such

connections may lead to further communications, files, or interactions that could establish the full scope of Valdez's involvement in these criminal activities.

28. There is probable cause to believe that the ACCOUNT's history and logs with metadata about Snaps, Stories, Chats will contain fruits, contraband, evidence, and/or instrumentalities of the specified offenses because these logs are likely to contain detailed records of communications, exchanges, and activities related to the production, distribution, and possession of child pornography, as well as the extortion and manipulation of minors. Given the documented use of the "cow_knees" Snapchat account to facilitate illegal activities, such as the sharing of explicit content and coercive interactions with minors, it is reasonable to believe that the history and logs will provide critical evidence of these illicit exchanges, too. The metadata, including timestamps, sender and recipient information, message status (whether opened or not), and any related media files, could help establish the timeline of the offenses and identify the individuals involved in these criminal activities. Additionally, any deleted or unsaved messages, including those in group chats or Stories, may provide further insights into ongoing attempts at exploitation and extortion. The history and logs could also reveal patterns of communication with other members of the criminal network, shedding light on the scope of the operation and the role of Valdez's "cow_knees" account in these

offenses. This evidence will be useful in linking the user of the account, Valdez, to the specified crimes and in identifying additional victims or co-conspirators.

29. There is probable cause to believe that the ACCOUNT's location data will contain fruits, contraband, evidence, and/or instrumentalities of the specified offenses because the location data can provide insights into the whereabouts of the individual behind the "cow_knees" account, believed to be Valdez, during the commission of the criminal activities. Given that Valdez has been involved in extorting minors and distributing child pornography, the location data may show patterns of movement or specific geographic areas linked to the commission of these offenses. For example, location data could reveal instances where Valdez was in proximity to certain victims, locations where illicit content was shared, or areas where he engaged in further criminal acts related to exploitation or coercion, including areas near geolocated IP addresses. Additionally, since the Snapchat app collects and retains location information when users opt in or during certain activities, the data may confirm interactions with specific individuals tied to the ongoing distribution and receipt of explicit material. The location history could also support or disprove statements made during the investigation, helping to establish a timeline of events and corroborating other evidence, such as the use of specific IP addresses linked to Valdez's criminal activities. Therefore, examining

this location data is useful in building a complete picture of how Valdez utilized digital platforms to facilitate his crimes.

30. There is probable cause to believe that the ACCOUNT's Memories content will contain fruits, contraband, evidence, and/or instrumentalities of the specified offenses. The Memories feature on Snapchat allows users to store images, videos, and messages that they wish to keep for longer periods of time, beyond the normal self-destructing nature of Snaps. Given that Valdez, through the "cow_knees" Snapchat account, has been involved in the distribution and possession of child pornography and the extortion of minors, it is likely that he used the Memories feature to preserve illicit content—like on his Maxtor SSD—including explicit images and videos of minors, as well as communications related to these criminal activities. Investigators have already identified that Valdez used encrypted storage and other secure means to retain evidence of his crimes, and it is consistent with his behavior to store valuable or incriminating materials in Snapchat's Memories (which can be encrypted under My Eyes Only, discussed below), where they can be easily accessed or shared at a later time. These stored items may include media files exchanged with other users or records of communications used to coerce minors into producing explicit material. The Memories content could thus provide critical evidence supporting the charges related to child exploitation, pornography, and extortion, and may reveal further

details about Valdez's involvement in these illegal activities, his interactions with other offenders, or the victims involved.

31. For similar reasons, there is probable cause to believe that the ACCOUNT's encrypted My Eyes Only content will contain fruits, contraband, evidence, and/or instrumentalities of the specified offenses. The "My Eyes Only" feature on Snapchat allows users to store sensitive or illicit materials in an encrypted, password-protected area. Given that Valdez, through the "cow_knees" Snapchat account, has been involved in the distribution and possession of child pornography, as well as the extortion and manipulation of minors, it is reasonable to believe that he used this secure storage feature to hide and protect illegal content, such as explicit images, videos, and communications related to his criminal activities. This content may include child pornography, coercive messages exchanged with minors, or evidence of his role in online extortion schemes. The use of encryption and password protection is consistent with behaviors seen in individuals involved in such crimes—including the "M.2 Container" belonging to Valdez—who often take steps to conceal and secure their illicit materials to avoid detection. Investigators may be able to access this content through forensic means, revealing critical evidence that could further substantiate the charges against Valdez and identify additional victims or co-conspirators involved in these criminal activities.

32. There is probable cause to believe that the ACCOUNT's search history content will contain fruits, contraband, evidence, and/or instrumentalities of the specified offenses because individuals involved in the production, distribution, and possession of child pornography, as well as sexual extortion, often conduct online searches for illicit materials, minors to exploit, and tools to facilitate their crimes. Given the documented connection between Valdez and the "cow_knees" Snapchat account to the creation and distribution of explicit content involving minors, it is likely that the search history will reveal queries related to interactions with other offenders, including searches for accounts where illegal content is exchanged. Furthermore, the search history is likely to contain username and account searches for persons "cow_knees" (Valdez) was seeking to exploit and cyberstalk in connection with the Discord activity. Examining this content could provide key evidence that links Valdez to the specified offenses and reveal additional steps in his criminal activities.

33. There is probable cause to believe that the ACCOUNT's "Our Story" and Crowd-Sourced Content will contain fruits, contraband, evidence, and/or instrumentalities of the specified offenses because, similar to how the Offending Server, including Duck (Valdez), previously conducted exploitation and blackmail operations through public internet spaces and groups, the "Our Story" feature on Snapchat and crowd-sourced content allow for the widespread sharing of illicit

material to a large, often anonymous, audience. In the case of the Offending Server, members of Extreme Group used these types of platforms to extort and coerce minors into producing explicit content, which was then shared within these public spaces to further the cycle of exploitation. Given Valdez's involvement in those activities, it is reasonable to believe that he used Snapchat's "Our Story" to distribute illegal content in a similar manner. Furthermore, Valdez's postings to "Our Stories" could provide critical evidence about his location at crucial moments in the timeline of this criminal case, particularly with respect to crimes committed behind a keyboard and over the Internet. The location data associated with posts to "Our Story" could show where Valdez was when he interacted with victims, shared illicit content, or conducted blackmail and extortion schemes. This geographic information could be pivotal in corroborating other evidence, such as IP addresses linked to criminal activity, and could further establish a clear link between criminal actions and Valdez.

34. Lastly, all of the above-specified service content for the ACCOUNT, including chat content, associated accounts, device information, Friends, history/logs, location data, Memories, My Eyes Only content, search history, and "Our Story" and crowd-sourced content, dating back to January 1, 2020, can provide critical attribution evidence regarding the who, what, where, when, and why of the digital devices used to commit the specified crimes. This comprehensive data set

will allow investigators to trace the specific actions and movements of the individual behind the "cow_knees" Snapchat account, believed to be Valdez, and establish clear links between the digital devices and criminal activities. By analyzing the device information, location data, and metadata, investigators can pinpoint when and where Valdez was engaging in criminal conduct, such as distributing child pornography, extorting minors, and communicating with other offenders. The Snap history, search history, and My Eyes Only content can help identify the types of illicit materials involved, the interactions with victims, and the methods used to further the criminal network. Additionally, the data from "Our Story" and crowd-sourced content could reveal the extent of Valdez's distribution efforts and provide a broader context for his activities within the criminal enterprise. The combination of this information will not only help reconstruct the timeline of events but also provide crucial evidence of intent, further establishing Valdez's role in the commission of these offenses and linking him to the digital infrastructure used in the exploitation and extortion of minors.

RELEVANCE OF SNAPCHAT DATA

35. Based on my training and experience, information stored in social media accounts—such as the ACCOUNT—often provides key evidence of the "who, what, why, when, where, and how" of criminal activity. This information can help prove each element of the offense or rule out individuals from suspicion.

Account data such as registration details, communications, images, videos, activity logs, timestamps, IP logs, and device information can identify who used the account at critical times. This type of user attribution is comparable to finding indicia of occupancy during the execution of a residential search warrant. Because, as demonstrated above, the ACCOUNT was used to carry out criminal activity—including the distribution, receipt, and possession of child pornography and extorting minors into producing child pornography—the full context of how the account was used is critical to attributing that criminal activity and understanding the user's role. It is not uncommon for criminal co-conspirators to share access to online accounts, making it essential to establish who actually used the account at relevant times.

36. As detailed above, in addition to preserving some content, Snapchat logs session times, device connections, IP addresses, location data, and user activity. This data is critical to help investigators place relevant conduct in chronological context and reconstruct a timeline of events. Shared content may contain embedded geolocation data or visual cues that can confirm where a user is located at a particular time. Metadata can show when files were uploaded, messages were sent, or content was viewed or deleted. Logs showing access from multiple devices may indicate the use of other phones, applications, or related accounts used to carry out the criminal activity.

37. Based on my training and experience, account content also tends to reflect the user's state of mind. Search history, deleted messages, or evidence of account manipulation—such as attempts to delete activity, rename the account, or change usernames—can reveal motive, intent, or consciousness of guilt. Such behavior may show that the user was aware of the criminal nature of their actions and took steps to conceal them. These digital actions are often just as telling as physical attempts to hide or destroy evidence and may provide valuable insight into the user's identity and intent.

38. Based on my training and experience, there is probable cause to believe the ACCOUNT contains evidence, fruits, contraband, and instrumentalities of the offenses under investigation, including child pornography production, distribution, receipt, and possession, extortion, and cyberstalking. For example, as detailed above, there is evidence that the user of the ACCOUNT possessed and distributed child pornography using Snapchat, and that other Snapchat users received child pornography from the user of the ACCOUNT. Similarly, there is evidence that the user of the ACCOUNT used Snapchat to discuss extorting minors into producing child pornography and that child pornography resulting from that extortion was produced, distributed, and received via Snapchat. Individuals who use a platform such as Snapchat to engage in crimes of this nature frequently use the same account to carry out additional related criminal activity, and relevant

evidence is commonly found in those accounts. In this case, Snaps, Stories, Memories, and Chats are all likely to contain such evidence because they are the primary ways users communicate, share media, and document their actions on Snapchat. Memories, for example, may contain media depicting child pornography and fan signs. Chats, for example, may contain communications where the user coerces victims into producing child pornography or creating fan signs, or brags about their conduct with co-conspirators. Stories, for example, may display material showcasing successful efforts to extort victims into producing such material. These features, taken together, are likely to contain probative evidence of the criminal activity under investigation.

39. Based on my training and experience, Snapchat data in the ACCOUNT is also likely to contain critical attribution evidence. This is particularly important when dealing with ephemeral platforms like Snapchat, where content is designed to disappear and user activity is often minimized or obscured. Device identifiers, login history, IP addresses, and location data can help confirm who accessed or controlled the account at relevant times. Content from Snaps, Chats, Memories, and other communications may help identify co-conspirators, victims, and reveal other accounts used by the same individual. A full review of the ACCOUNT's content and non-content data will provide valuable context for establishing attribution, intent, and understanding the broader scope of

the offenses under investigation, as well as the identification of additional victims and co-conspirators.

40. Lastly, should Snap possess no (or limited) information for the above-specified services on the ACCOUNT, there is probable cause that such a response from Snap would constitute evidence that the ACCOUNT owner—Rumaldo Valdez—deleted or tampered with his ACCOUNT data after the May 31, 2024 search warrant operation, thus obstructing this investigation. Relevant to that conclusion are the multiple attempted logins from a Mililani IP address, noted above, following the May 31, 2024 search warrant operation. Comparing the "cow_knees" Snap data on the iPhone 14 with the information provided pursuant to this warrant would enable investigators to determine whether the ACCOUNT data was tampered with or deleted following the May 31, 2024 search warrant operation, before the November 19, 2024 data preservation request.

CONCLUSION

41. Based on the foregoing, I request that the Court issue the proposed search warrant.

42. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving it on Snap Inc. Because the warrant will be served on Snap, who will then compile the requested records at a time convenient

to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR SEALING

43. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

Respectfully submitted,

Kyle Charles Rawlinson
Special Agent
Federal Bureau of Investigation

Sworn to under oath before me telephonically, and attestation acknowledged pursuant to Fed. R. Crim. P. 4.1 (b)(2), this 14 day of May 2025, at Honolulu, Hawaii.

Wes Reber Porter
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

This warrant applies to information (in any format) associated with each of the following accounts/identifiers:

cow_knees

(the "Account") that is stored at premises owned, maintained, controlled, or operated by Snap Inc., a company headquartered at 2772 Donald Douglas Loop North, Santa Monica, CA 90405.

ATTACHMENT B

Particular Things to Be Seized

I. Information to be disclosed by Snap Inc. ("Snap"):

To the extent that the information described in Attachment A is within the possession, custody, or control of Snap, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Snap, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Snap is required to disclose to the government for the Account or identifiers listed in Attachment A the following information, unless otherwise indicated:

a. All business records and subscriber information, in any form kept, pertaining to the Account, including:

1. Names (including legal names, subscriber names, Snapchat usernames, and vanity names);

2. Addresses (including mailing addresses, residential addresses, business addresses, and email addresses, including alternate and recovery email addresses);

3. Whether Maps and/or two-factor-authentication are enabled.

4. Telephone numbers, including SMS recovery and alternate sign-in numbers;

5. Records of session/connection times and durations (including longs and logouts), and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions/ connections, including log-in IP addresses, and methods of connection;

6. Telephone or instrument numbers or other subscriber numbers or identities, including any temporarily assigned network address, SMS recovery numbers, voice numbers, and alternate sign-in numbers;

7. Length of service (including start date and creation IP), types of service utilized, last active date, and app versions;

8. Means and source of payment (including any credit card or bank account number); and

9. Change history, including all information pertaining to creation of the Account, such as date and time of creation, IP address used to create the Account, and all subscriber information provided at the time the Account was created.

b. All stored communications and other files in Snap's possession for the Account, whether physical, stored on electronic media, or temporarily extant on any computer or server, reflecting communications to or from the Account, including the content of all messages and Snaps sent, received, and saved, stored, or preserved;

c. Records of the Account's device information, details about the devices used to access the Snapchat service (brands, model numbers), IP addresses, device identifiers (IMEI), operating system, location data, and associated metadata;

d. Records of the Account's address books, contact lists, and "friends";

e. Records of other user accounts associated with, referenced in or accessed by the Account, as well as the account name, vanity name, identifiers, and all available subscriber information (paragraph a, above) for any other Snapchat account(s) associated with the Account;

f. History and logs for the Account, including those containing metadata about Snaps, Stories, and Chats, as well as Logs of all messages and all files that have been created, and Snaps sent/or accessed via the Account, or that are controlled by accounts associated with the Account;

g. Files and system attributes (and records thereof) accessed, modified, or added by the Account's user, particularly Memories content and My Eyes Only content;

h. Records of the Account's location data, including timestamps, geographic (GPS) coordinates, and associated metadata;

i. Records of the Account's search history, including keywords, search terms, and associated metadata; and

j. Records of the Account's "Our Story" and crowd-sourced content, including uploads, timestamps, metadata, and interactions with other users.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and/or instrumentalities of violations of 18 U.S.C. §§ 371 (Conspiracy), 1951 (Extortion), 2251 (Production of Child Pornography), 2252A (Distribution, Receipt, and Possession of Child Pornography), 2261A (Cyberstalking), and 1512 (Obstruction of Justice), those violations involving Rumaldo Valdez and others, and occurring on or after January 1, 2020, including, for each Account or identifier listed on Attachment A, information pertaining to the following matters:

a. Production, distribution, receipt, and/or possession of child pornography, and any conspiracy to commit the same;

b. Cyberstalking over the Internet (i.e., causing or attempting to cause substantial emotional distress to another person, or placing that person in reasonable fear of death of or serious bodily injury, through a course of conduct with intent to kill, injure, harass, intimidate) and conspiracy to commit the same;

c. Extortion over the Internet (i.e., obtaining a victim's property with the victim's consent, by the actual or threatened wrongful use of force, violence, or fear, including fear of economic loss) and conspiracy to commit the same;

d. Deletion of, or others actions obstructing the investigation into, data for the Account and/or any Discord accounts using variants of the moniker "Duck" (including, but not limited to, Discord accounts "Duck.#8030" and "Duck..#8030");

e. Use and control of accounts using variants of the moniker "Duck" (including, but not limited to, Discord accounts "Duck.#8030" and "Duck..#8030");

f. Participation and access to the online groups, including extremist collectives on Discord servers, that produce and/or share child pornography, extort minors into creating self-harm material and/or child pornography, and distribute such content within and outside of the group;

g. Use and control of the IP address 75.80.178.28;

h. The unauthorized access of the Account;

i. The whereabouts of Valdez at the times under investigation

j. Evidence indicating how and when the Account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

k. Evidence indicating the Account owner's state of mind as it relates to the crime under investigation;

l. The identity of the person(s) who created or used the Account, including records that help reveal the whereabouts of such person(s).

m. The identity of the person(s) who communicated with the Account about matters relating to child pornography, cyberstalking, and extortion, including records that help reveal their whereabouts.

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.