

UNITED STATES DISTRICT COURT

for the

District of Hawaii

FILED IN THE
UNITED STATES DISTRICT COURT
DISTRICT OF HAWAII
May 16, 2025 8:46 AM
Lucy H. Carrillo, Clerk of Court

United States of America

v.

RUMALDO VALDEZ

Case No. MJ25-564 WRP

Defendant(s)

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

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of May 31, 2024 in the county of Honolulu in the
District of Hawaii, the defendant(s) violated:

*Code Section**Offense Description*

18 U.S.C. § 2252(a)(4)(B)

Knowingly possessing a visual depiction of a minor engaged in sexually explicit conduct, with said visual depiction having travelled in or affected interstate or foreign commerce

18 U.S.C. § 2252A(a)(5)(A)

Knowingly possessing any material containing child pornography, while in the special maritime and territorial jurisdiction of the US or US government land

18 U.S.C. § 2252A(a)(1)

Knowingly mailing, transporting, or shipping child pornography, using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce

This criminal complaint is based on these facts:

See attached affidavit.

☒ Continued on the attached sheet.


Complainant's signature

FBI SA Scott Wells

Printed name and title

Sworn to under oath before me telephonically, and attestation
acknowledged pursuant to Fed.R.Crim.P. 4.1(b)(2).

Date: May 16, 2025City and state: Honolulu, Hawaii


Wes Reber Porter
United States Magistrate Judge

KENNETH M. SORENSON
Acting United States Attorney
District of Hawaii

WAYNE A. MYERS
JONATHAN D. SLACK
Assistant U.S. Attorneys
Room 6100, PJKK Federal Building
300 Ala Moana Blvd.
Honolulu, Hawaii 96850
Telephone: (808) 541-2850
E-mail: Wayne.Myers@usdoj.gov
Jonathan.Slack@usdoj.gov

Attorneys for Plaintiff
UNITED STATES OF AMERICA

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF HAWAII

UNITED STATES OF AMERICA,

Plaintiff,

vs.

RUMALDO VALDEZ,

Defendant.

Case No. MJ25-564 WRP

AFFIDAVIT IN SUPPORT OF
CRIMINAL COMPLAINT

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT

I, the undersigned complainant, being duly sworn telephonically, state the following is true and correct to the best of my knowledge and belief:

INTRODUCTION

1. This affidavit is made for the purpose of establishing probable cause that, on or about May 31, 2024 within the District of Hawaii and elsewhere, RUMALDO VALDEZ (1) knowingly possessed one or more visual depictions of a minor engaged in sexually explicit conduct,¹ with such visual depiction(s) having been mailed, shipped, or transported in interstate or foreign commerce by any means, including by computer, in violation of Title 18, United States Code, Section 2252(a)(4)(B); (2) knowingly possessed any computer disk or any other material that contains an image of child pornography,² while in the special maritime and territorial jurisdiction of the United States³ or on any land or building owned by, leased to, or otherwise used by or under the control of the United States Government, in violation of Title 18, United States Code, Section 2252A(a)(5)(A); and (3) knowingly mailed,

¹ “Sexually explicit conduct” means actual or simulated sexual intercourse, bestiality, masturbation, sadistic or masochistic abuse, or lascivious exhibition of the genitals or pubic area of any person. *See* 18 U.S.C. § 2256(2). The defendant must know that each visual depiction shows a minor engaged in sexually explicit activity. *See United States v. Lacy*, 119 F.3d 742, 747 (9th Cir. 1997).

² For this affidavit, the Court need not consider the “computer generated” component of the “child pornography” definition, 18 U.S.C. § 2256(8)(B), because each of the images described below appears to your Affiant to contain “visual depiction[s] involv[ing] the use of a minor engaging in sexually explicit conduct,” *id.* § 2256(8)(A). A “minor” is any person under 18 years of age. *Id.* § 2256(1).

³ “Special maritime and territorial jurisdiction of the United States” includes United States military installations. *See United States v. Torres*, 2006 WL 3826793, at *6 (D. Haw. Dec. 27, 2006).

transported, or shipped child pornography, using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce by any means,⁴ including by computer, in violation of Title 18, United States Code, Section 2252A(a)(1).

2. I am a Special Agent assigned to the Federal Bureau of Investigation (“FBI”) Honolulu Division Joint Terrorism Task Force. I have completed law enforcement training courses at the FBI Training Academy at Quantico, Virginia, and have executed federal search and arrest warrants. I investigate criminal violations relating to child exploitation and child pornography, including violations pertaining to the illegal production, distribution, receipt, and possession of child pornography. I have worked with other federal agents, as well as state and local law enforcement officers, who have shared with me their knowledge and experience regarding child pornography investigations. I have experience identifying distinguishing features of children at various stages of development, such that I can reasonably determine ages of minors depicted in visual media.

3. The facts in this affidavit come from my observations, my training and experience, and information obtained from other law enforcement agents. This

⁴ Knowingly transporting child pornography across state lines is sufficient. *See, e.g., United States v. Wright*, 625 F.3d 583, 593 (9th Cir. 2010), *superseded by statute on other grounds*, Pub. L. 110-401, Title III, § 304, Oct. 13, 2008, 122 Stat. 4242; *United States v. Welton*, 2009 WL 4507744, at *8 (C.D. Cal. Nov. 30, 2009).

affidavit is intended to show that there is sufficient probable cause for the offenses specified above and does not set forth all of my knowledge about this matter. Throughout this affidavit, I use square brackets “[]” to anonymize personal identifiers and investigation-sensitive usernames.

PROBABLE CAUSE

4. In 2021, law enforcement received CyberTips from the National Center for Missing and Exploited Children (“NCMEC”) reporting that members of a particular Discord server (hereinafter, “Offending Server”) were producing and sharing child sexual abuse material. The FBI began investigating members of that server, including variants⁵ of the username “Duck” (e.g., “Duck.#8030”) and “M[username],” for child pornography offenses and for extorting minors into self-harm and sexual abuse.

5. In 2024, a Confidential Human Source (“CHS”)⁶ admitted to the FBI that the CHS had participated with Offending Server members in extorting minors into creating self-harm material and child pornography. According to the CHS, server members—including a member going by the moniker “Duck”—would send

⁵ In my training and experience, I know it is common for Discord users, after having a particular account banned for prohibited activity on the platform, to create new account usernames with minor variations from their old username(s). This permits alias persistence.

⁶ At the time of the CHS’s statements, the CHS was seeking lenience from the government in connection with sentencing.

victims links to malicious files that, if clicked on by the victims, would deploy malware on victims' computers that the server members could then use to accomplish blackmail. The CHS described "Duck" as an active member of the Offending Server and, around the time of the CHS's participation in the group, knew "Duck" to be operating somewhere near Oceanside, California. The CHS reported having witnessed "Duck" coerce a minor female, approximately 14 to 16 years old, into recording a masturbation video. "Duck" later used that masturbation video to blackmail the minor into recording and sharing a cutting video in which she cut "Duck" into her arm, according to the CHS. "Duck" later promoted the video online, also according to the CHS. In my experience investigating the Offending Server and similar online groups, I know that participants in such groups often collect victim "fan signs" (media) as trophies from their online extortions and championing their aliases.

6. Some of the 2021 NCMEC CyberTips listed "Duck.#8030" as having uploaded child pornography to Discord. Investigators identified "Duck.#8030" as RUMALDO VALDEZ through, among other connective evidence, an IP address ending in -178.28 and an email address "boobuh[number]@gmail.com," both provided by Discord for "Duck.#8030," and both associating with a "Rumaldo Valdez" in records returned by the internet service provider and Google, respectively. The recovery phone number in Google's records matched the listed

phone number for a Navy Petty Officer Third Class “Rumaldo Valdez.” The billing address in the internet service provider’s records matched the “Home of Record” listed for that same Navy PO3 “Rumaldo Valdez.”⁷

7. On May 31, 2024, investigators executed a federal 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.⁸ While examining the SanDisk SSD, investigators encountered a virtually encrypted container titled, “M.2 Container.” And while

⁷ The billing address is located within, and the -178.28 IP address geolocates to, San Diego County, California. This corroborates the CHS’s reporting that “Duck” was operating near Oceanside, California, also within San Diego County.

⁸ The “duckk” email address was associated with a child pornography CyberTip on Discord user “Duck#8030,” not summarized above.

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.”

8. 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.

9. 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 8, 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.”

10. 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.

11. 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-character 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.

12. 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 in the preceding paragraph. There is thus probable cause to believe that the image is child pornography and that VALDEZ knowingly mailed, transported, or shipped *at least* that child pornography image across state lines, into the District of Hawaii.

13. 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.

CONCLUSION

14. Based on the foregoing facts and my training and experience, I respectfully submit that probable cause exists to believe VALDEZ committed the aforementioned offenses.

Respectfully submitted,



Scott Wells
Special Agent
Federal Bureau of Investigation

This Criminal Complaint and Affidavit in support thereof were presented to, approved by, and probable cause to believe that the defendant above-named committed the charged crime found to exist by the undersigned Judicial Officer at XXXXXXXXXXXXXX on May 16, 2025.

Sworn to under oath before me telephonically and attestation acknowledged pursuant to FRCP 4.1(b)(2), on May 16, 2025, at Honolulu, Hawaii.



Wes Reber Porter
United States Magistrate Judge