AO 91 (Rev. 11/11) Criminal Complaint (Rev. by USAO on 3/12/20) ☐ Original ☐ Duplicate Original

UNITED STATES DISTRICT COURT

for the

Central District of California

United States of America,

v.

Sagi Schwartzberg,

Defendant.

Case No. 5:21-mj-00317

CRIMINAL COMPLAINT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

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

Between the date(s) of May 13, 2020 and December 10, 2020, in the counties of Los Angeles and San Bernardino in the Central District of California, the defendant violated:

Code Section	*Offense Description*
18 U.S.C. § 2251(a)	Production of Child Pornography

This criminal complaint is based on these facts:

Please see attached affidavit.

☒ Continued on the attached sheet.

/s/ pursuant to Fed. R. Crim. P. 4.1
Complainant's signature

L.M. Wall, FBI Special Agent
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: April 27, 2021

Judge's signature

City and state: Riverside, California

Hon. Kenly Kiya Kato, U.S. Magistrate Judge
Printed name and title

AUSA: Sonah Lee x26924

AFFIDAVIT

I, LISA M. WALL, being duly sworn, declare and state as follows:

I. BACKGROUND OF AFFIANT

1. I am a Special Agent with the Federal Bureau of Investigation and have been so employed since June of 2004. I am currently assigned to the Violent Crimes Squad of the Los Angeles Field Office, where I primarily investigate crimes involving child exploitation and the receipt, possession, advertisement, transmission, and production of child pornography. I am a member of the Inland Regional Child Exploitation and Human Trafficking Task Force and of the Riverside County Internet Crimes Against Children/Sexual Assault Felony Enforcement Team, which investigates such cases.

2. My experience as an FBI Special Agent includes investigating the use of computers and the Internet to commit crimes. I have received training and gained experience in interviewing and interrogation techniques, arrest procedures, search warrant applications, the execution of searches and seizures, computer crimes, computer evidence identification, child pornography identification, computer evidence seizure and processing, and various criminal laws and procedures. I have personally participated in the execution of search warrants involving the search of social media accounts, email accounts, and the search and seizure of computer equipment.

3. Through my training and experience, I have become familiar with the methods of operation used by people who sexually exploit children. I have received specialized training

in the areas of computer crimes, child pornography, and the sexual exploitation of children on the Internet. This training, and my experience in these investigations, have given me an understanding of how people involved with offenses concerning the sexual exploitation of children use the Internet to further those offenses. Additionally, I have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in numerous forms of media, including on computers and digital devices. I have personally conducted and participated in numerous authorized searches, including those specifically involving investigations of the production of child pornography, distribution of child sexual assault material via peer-to-peer networks, and other violent crimes against children.

II. PURPOSE OF AFFIDAVIT

4. This affidavit is made in support of a criminal complaint against SAGI SCHWARTZBERG ("SCHWARTZBERG") and arrest warrant for violations of 18 U.S.C. § 2251(a)(Production of Child Pornography).

5. The facts set forth in this affidavit are based on my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint and warrants and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically

indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

III. DEFINITIONS

6. The following definitions apply to this affidavit:

a. "Minor," "sexually explicit conduct," "visual depiction," and "child pornography" are defined as set forth in Title 18, United States Code, Section 2256. The term "computer" is defined as set forth in 18 U.S.C. § 1030(e)(1).

b. "Child erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors, but that are not necessarily obscene or do not necessarily depict minors in sexually explicit poses or positions.

c. "Computer" is defined as set forth in Title 18, United States Code, Section 1030(e)(1).

d. "Computer hardware" consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices, including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices; peripheral input/output devices, including keyboards, printers, video display monitors, and related communications devices such as cables and connections; and any devices, mechanisms, or parts that can be used to restrict access to computer hardware, including physical keys and locks.

e. "Email" (electronic mail) is the messages/content sent from one person to another via a computer or another digital device or means. Email may also include files sent as attachments to or embedded within text messages. Email can be sent automatically to a large number of digital addresses via a mailing list.

f. "Internet" is the worldwide network of computers. It is a noncommercial, self-governing network devoted mostly to communication and research with roughly 4.57 billion users worldwide. The Internet is not an online service and has no central hub. It is a collection of computer networks, online services, and single user components. In order to access the Internet, an individual computer or digital device user must use an access provider, such as a university, employer, or commercial Internet Service Provider ("ISP"), which operates a host computer with direct access to the Internet.

g. "Internet Protocol" ("IP") is the primary protocol upon which the Internet is based. IP allows a digital packet of information to travel through multiple networks (groups of linked computers) on the way to its ultimate destination.

h. "Internet Protocol address" or "IP address" refers to a unique number used by a computer or other digital device to access the Internet. IP addresses can be "dynamic," meaning that the Internet Service Provider, as defined below, assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be "static," if

an Internet Service Provider assigns a user's computer a particular IP address that is used each time the computer accesses the Internet.

i. ISP is a business that allows a user to dial into or link through its computer or digital devices thereby allowing the user to connect to the Internet, often for a fee. ISPs generally provide an Internet connection, an electronic mail address, and, sometimes, Internet browsing software. A user can also connect to the Internet through a commercial online service such as AT&T, Verizon, or Time Warner Cable. With this kind of connection, the user gets Internet access and the proprietary features offered by the online service, such as chat rooms and searchable databases.

j. "Jpeg," "jpg," "gif," "bmp," and "art" are graphic image files, namely, pictures.

k. "Mpeg," "mpg," "mov," "avi," "rm," and "wmv" are video files. To use these video files, one needs a personal computer or other digital device with sufficient processor speed, internal memory, and hard disk space to handle and play typically large video files. One also needs a video file viewer or client software that plays video files. One can download shareware or commercial video players from numerous sites on the Internet.

l. "Records," "documents," and "materials," include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

IV. SUMMARY OF PROBABLE CAUSE

7. In November 2020, MediaLab Inc., previously known as Kik Interactive Inc. ("Kik"), an American-based instant messaging application for mobile devices, submitted a Cybertip to National Center for Missing and Exploited Children ("NCMEC") that one of its users, "drunkesq_o64" was identified as uploading and sharing suspected child pornography on Kik. Kik provided registration information and login records that show that "drunkesq_064" was registered with the email address of sagi.schwartzberg@gmail.com (the "SUSPECT EMAIL") and had uploaded suspected child pornography from IP address 66.146.71.106 ("SUSPECT IP 1") and from IP address 99.23.173.186 ("SUSPECT IP 2").

8. The information was subsequently sent to the Fontana Police Department Internet Crimes Against Children Task Force ("FPD ICAC"), for further investigation. The FPD ICAC subsequently learned that the SUSPECT IP 1 was assigned to the service account at Schwartzberg & Luther, APC, with a billing address of 3125 E. Guasti Road, Ontario, California. The FPD ICAC also learned that SUSPECT IP 2 was assigned to a Sagi Schwartzberg (later identified as SCHWARTZBERG) at the residence at 14179 Dartmouth Court, Fontana, California ("SUSPECT RESIDENCE").

9. FPD ICAC conducted surveillance at SUSPECT RESIDENCE to confirm that SCHWARTZBERG resides at SUSPECT RESIDENCE.

10. On February 17, 2021, members of the FPD ICAC executed a state residential search warrant at the SUSPECT RESIDENCE,

along with a Special Master appointed by the Count of San Bernardino.

11. FPD detained SCHWARTZBERG and interviewed him. SCHWARTZBERG admitted that "sagi.schwartzberg@gmail.com" was his email address. SCHWARTZBERG also admitted that he had previously shared child pornography in a Kik group chat.

12. During the search of the SUSPECT RESIDENCE, FPD ICAC located an iPhone X, SN-FK1W2UWRJCL6, which contained a hidden vault application containing file folders that were titled with names of females. Specifically, one folder that was labeled as "Mxxxx"[1] contained sexually explicit images and videos of a minor female who appeared to be between 13-15 years old.

13. FPD ICAC was able to locate and interview the minor female ("MV 1") whose images were found in the "Mxxxx" folder in SCHWARTZBERG's cell phone. MV 1 is currently a 15 year old female who stated that she began messaging with a SnapChat screen name of "Jason D" and user ID of "xocdrunkx," later identified as SCHWARTZBERG, via SnapChat about two years ago. MV 1 stated that SCHWARTZBERG was aware that she was a minor, and paid her in Vanilla e-gift cards for her to send him sexually explicit photos and videos of herself to him via SnapChat. MV 1 was aware that SCHWARTZBERG had saved her photos and videos on his end by taking a screenshot because SnapChat notifies her when someone takes a screenshot of any image that she posts or sends.

---

[1] The name of this folder has been shortened and anonymized to protect the identity of the minor witness.

14. FPD ICAC, with assistance from FBI, has identified several other minor females whose sexually explicit images were located on SCHWARTZBERG's cell phone, and is currently attempting to locate and interview them.

V. STATEMENT OF PROBABLE CAUSE

A. Background on CyberTips and NCMEC

15. NCMEC was established in 1984 as a private, nonprofit 501(c)(3) organization. NCMEC provides services nationwide for families and professionals in the prevention of abducted, endangered, and sexually exploited children. Pursuant to its mission and its congressional authorization (see 42 U.S.C. § 5773), NCMEC operates the CyberTipline and the Child Victim Identification Program to assist law enforcement in identifying victims of child pornography and child sexual exploitation. NCMEC works with law enforcement, Internet service providers, electronic payment service providers, and others to reduce the distribution of child sexual exploitation images and videos over the Internet. NCMEC's CyberTipline is the nation's centralized reporting system for the online exploitation of children. The public and electronic service providers can make reports of suspected online enticement of children for sexual acts, extra-familial child sexual molestation, child pornography, child sex tourism, child sex trafficking, unsolicited obscene materials sent to a child, misleading domain names, and misleading words or digital images on the internet. NCMEC does not investigate and cannot verify the accuracy of information reported to NCMEC. NCMEC forwards the reports of child sexual exploitation to law

enforcement for purposes of investigation and disposition of potential criminal wrongdoing to be determined solely by the relevant law enforcement agency and prosecutor's office. As part of the CyberTipline program, internet service providers that identify suspected child exploitation material on their systems may send a report to NCMEC. The reports contain information such as the account name, name, telephone number, and ISP address associated with an individual who uploaded suspected child exploitation material. The CyberTipline reports also indicate whether the provider viewed the suspected child exploitation material.

B. Background on Kik

16. Kik is a mobile application designed for chatting or messaging. Prior to October 2019, Kik was owned and operated by Kik Interactive, Inc., a Canada-based company operating from Ontario, Canada. In October 2019, Kik was acquired by MediaLab, a multimedia company based in Los Angeles, California.

17. According to the publicly available document, "Kik's Guide for Law Enforcement," to use this application, a user downloads the application to a mobile phone, computer, or other digital device via a service such as the iOS App Store, Google Play Store, Apple iTunes, or another similar provider. Once the application is downloaded and installed, the user is prompted to create an account or login to an existing account by entering the Kik username or email address and the necessary password. To create a Kik account, users are prompted to enter their first name, their last name, a Kik username, their email address,

password, and their date of birth. Kik does not verify that the information entered is valid. For example, Kik does not verify that the email address entered is valid or that the birthday entered is the user's actual birthday. Kik allows for the entry of a phone number upon registering but it is not required.

18. Once the user has created an account, the user is able to locate other users via a search feature. While messaging, users can then send each other text messages, images, and videos.

19. According to "Kik's Guide for Law Enforcement," Kik users are also able to create chat groups with a limited number of individuals to communicate in a group setting and exchange text messages, images, and videos. These groups are administered by the group creator who has the authority to remove and ban other users from the created group. Once the group is created, Kik users have the option of sharing a hyperlink which serves as an invitation to the group. The Kik groups are identified by a hashtag (#) followed by the name of the group. For example, "#Sports" would be used to identify a Kik group for people interested in discussing or sharing information about sports.

20. According to Kik's Law Enforcement Response Team, Kik's Terms of Service prohibit users from uploading, posting, sending, commenting on, or storing content that contains child pornography and/or child abuse images. The Terms of Service also provide that Kik may review, screen and delete user content at any time if Kik believes use of their services are in

violation of the law. According to Kik, Kik has a strong business interest in enforcing their Terms of Service and ensuring that their services are free of illegal content, and in particular, child sexual abuse material. Accordingly, Kik reports that it independently and voluntarily takes steps to monitor and safeguard their platform and that ridding Kik products and services of child abuse images are critically important to protecting their users, product, brand, and business interests.

21. According to information provided by Kik, Kik is mandated by federal law to report to NCMEC any images and/or videos that would constitute suspected child pornography which are discovered on the Kik platform. Kik identifies child pornography in various ways and trains its employees to report apparent child pornography. Kik voluntarily makes reports to NCMEC in accordance with that training. After Kik discovers the suspected child pornography, Kik removes the content from its communications systems and closes the user's account.

C. Background on Snapchat

22. Snapchat, like Kik, is a mobile application designed for chatting or messaging. Snapchat is owned and operated by Snap Inc., a company operating from Santa Monica, California. When messages or "snaps" are sent over the Snapchat network they are able to be opened and viewed by the recipient Snapchat user. Once the snap is opened, it remains viewable for a period of one to ten seconds (exact time is decided by the sender) before the snap is permanently deleted from the recipient's account. In

this way, Snapchat users can send one-time, expiring messages to each other that contain photos and text.

23. A recipient Snapchat user can save a snap by taking a screenshot of the snap. When a recipient Snapchat user takes a screenshot of the snap, Snapchat notifies the sending Snapchat user.

D. Kik User "Drunkesq" Is Suspected of Uploading Child Pornography

24. In November 2020, FPD ICAC received NCMEC CyberTip Report 82985107 that Media Lab Inc., formerly known as Kik, ("Kik") forwarded to NCMEC on November 20, 2020. On or about December 28, 2020, FPD ICAC Detective Justin Moyer reviewed the report and found that Kik provided Information relating to a Kik account "drunkesq_o64" (account herein referred to as "drunkesq"). The information from Kik included a Subscriber Data Report containing registration information, email address and login records for an "drunkesq," a copy of the uploaded child pornography images and videos, and a report containing information detailing the date and time the child pornography images were uploaded and from which IP address they had been uploaded from.

25. Detective Moyer reviewed the Subscriber Data Report and learned that "Drunkesq" had uploaded suspected child pornography from SUSPECT IP 1 on October 28, 2020, at 22:23:49 UTC, and from SUSPECT IP 2 on November 15, 2020, at 16:01:40 UTC.

26. The NCMEC Report also provided the following registration information:

First Name: Drunk

Last Name: Esq

Email: sagi.schwartzberg@gmail.com (unconfirmed)

27. I reviewed the suspected child pornography files uploaded by "drunkesq" which were forwarded to NCMEC by Kik and found that these files depict prepubescent girls who appear to be between the age of 6 to 10 years old, displaying their vaginal and anal regions and/or engaged in vaginal and anal sex with adult men, as well as one image which appears to be child erotica.

a. Specifically, one video file titled, "5a7cb53e-da9e-48c3-8813-7bfaf0b08893.mp4" depicts a prepubescent girl, who appears to be between the ages of 6-9 years old. She is lying on her back, wearing a navy-blue t-shirt and naked from the waist down. An adult man wearing red shorts pushed her legs up to her chest and his erect penis is inserted into the child's anus. The video is approximately 30 seconds in duration and the camera angle focuses on the anal penetration, then the child's face. The child grunts as if in pain, has her eyes closed and is grimacing. The CyberTip Report accompanying the child pornography video reported that the image was uploaded by "drunkesq" on October 28, 2020, at 22:23:33 (UTC) from SUSPECT IP 1.

b. I reviewed an image titled "b25e3ef3-d6e3-4db4-b24f-a00fcb1cca04.jpg," which appears to be child erotica

depicting a prepubescent girl between the ages of 6-10 years old. The child is lying on her back with her legs spread apart and pulled up to her chest. She appears to be wearing thong-type underwear. The CyberTip Report accompanying the child erotic image reported that the image "b25e3ef3-d6e3-4db4-b24f-a00fcb1cca04.jpg," was uploaded by "drunkesq," at 16:01:40 UTC on November 15, 2020, from SUBJECT IP 2.

E. Identification Sagi SCHWARTZBERG

28. On or about December 29, 2020, Detective Moyer searched the website Maxmind.com - an online search tool used to identify the Internet service provider owning a specific IP address – for the SUSPECT IP 1. Detective Moyer learned that the SUSPECT IP 1 is owned by Ultimate Internet Access Inc. Detective Moyer served a state search warrant to Ultimate Internet Access seeking subscriber information for the SUSPECT IP 1. In response, Detective Moyer received information that SUSPECT IP 1 was assigned to service at the law office of Schwartzberg & Luther, APC, at 3125 E. Guasti Rd., Ontario, California 91761.

29. Detective Moyer also determined that the SUSPECT IP 2 was assigned to AT&T. Detective Moyer served a state search warrant to AT&T for subscriber information associated with the SUSPECT IP 2. In response, Detective Moyer received information from AT&T that the SUSPECT IP 2 was assigned to Sagi SCHWARTZBERG at 14179 Dartmouth Court, Fontana, California "SUSPECT RESIDENCE"). The email associated with the internet service at SUSPECT IP 2 was "sagi.schwartzberg@hotmail.com."

The account was established July 7, 2016, and was current as of January 1, 2021.

30. On or about December 29, 2020, Detective Moyer sent a state search warrant to Google, requesting information associated with "sagi.schwartzberg@gmail.com, the email account associated with Kik account "drunkesq", including subscriber information, messages, photos, videos, and other information associated with the account between October 20, 2020, through December 29, 2020.

31. On or about January 5, 2021, Google responded to the state search warrant and provided the information requested by the search warrant. Amongst the information provided by Google was that the recovery email address for the gmail email account was "sagi.schwartzberg@hotmail.com," and telephone number 818-271-9941. The "sagi.schwartzberg@gmail.com" was created on November 9, 2007. No images or chats were in the searched account.

32. Using a law enforcement database, Detective Moyer confirmed that telephone number 818-271-9941 was assigned to, or associated with, Sagi SCHWARTZBERG.

33. A search of the California Department of Motor vehicles for SCHWARTZBERG determined that SCHWARTZBERG had identified SUSPECT RESIDENCE as his residential address.

34. In January 2021, FPD ICAC team members conducted surveillance at the SUSPECT RESIDENCE and observed several vehicles registered to SCHWARTZBERG parked at the SUSPECT RESIDENCE.

F. Kik Account "Hoping4achance" Is Suspected of Uploading Child Pornography

35. In January 2021, Detective Moyer learned that another NCMEC Cybertip Report 64297739 had been forwarded to the San Bernardino County Sheriff's Department, Rancho Cucamonga Office ("SBSD") in February 2020, which appeared to also involve SCHWARTZBERG. Detective Moyer was provided with a copy of the CyberTip and the images and videos associated with this Cybertip.

36. SBSD received NCMEC CyberTip Report 64297739 that Kik forwarded to NCMEC on February 10, 2020. Detective Moyer reviewed the report and found that Kik provided information relating to the Kik user account ID "hoping4achance_rz6" with associated email account hoping4achance@yahoo.com and username of "hoping4achance" (account referred to as "hoping4achance"). The information from Kik included a Subscriber Data Report containing registration information, email address and login records for "hoping4achance," a copy of the uploaded suspect child pornography images and videos, and a report containing information detailing the date, time, and IP address the suspect child pornography images were uploaded from.

37. Detective Moyer reviewed the Subscriber Data Report and learned that "hoping4achance" had uploaded suspected child pornography from SUSPECT IP 2, on February 5, 2020.

38. Detective Moyer reviewed the child pornography video uploaded by "hoping4achance" which were forwarded to NCMEC by

Kik and found the video uploaded from the SUSPECT IP 2 depicted child pornography.

a. Specifically, one video titled, "e31f4bb7-a9ef-4208-9231-e7a5e11dbf0b.mp4," approximately 1 minute and 18 seconds in length, depicted a prepubescent child lying on a bed sleeping. The only thing showing is her face against a Little Mermaid bedsheet. An adult erect penis is shown inches away from her open mouth and the male begins to masturbate to the point of ejaculating into the young girl's mouth. This video appears to be a compilation depicting the same acts performed on a young girl at different times.

G. Search of SUSPECT RESIDENCE and Interview of SCHWARTZBERG

39. On February 11, 2021, the Honorable Joseph Ortiz, Judge of the Superior Court of California, County of San Bernardino issued a California state search warrant for the SUSPECT RESIDENCE.

40. On February 17, 2021, members of the FPD ICAC team, along with a Special Master appointed by the court[2], executed a state search warrant at the SUSPECT RESIDENCE. At that time,

[2] Pursuant to California Penal Code, Section 1524, a court shall appoint a special master to accompany law enforcement when serving a search warrant when the search warrant is issued for any documentary evidence in the possession or control of any person who is a lawyer as defined in California Evidence Code Section 950, a physician as defined in California Evidence Code Section 990, a psychotherapist as defined in California Evidence Code Section 1010, or a member of the clergy defined in California Evidence Code Section 1030.

SCHWARTZBERG was present at the home along with his wife and young children.

41. FPD ICAC detained SCHWARTZBERG and interviewed him. SCHWARTZBERG, in a recorded and Mirandized interview, admitted that "sagi.schwartzberg@gmail.com" (the email that was associated with the Kik account "drunkesq") belonged to him, but initially denied having a Kik account. When asked if he had any child pornography saved onto his iPhone, SCHWARTZBERG stated, "not that I am aware of, I have girls that I know, but they're over 18." When FPD ICAC described the child pornography videos and images from Cybertip Report 82985107 to SCHWARTZBERG, SCHWARTZBERG requested to sit down, then placed his hands over his face and appeared as if he were crying.

42. SCHWARTZBERG then admitted that he never used his any of his computers for "any of that" and that if law enforcement had evidence that that someone had uploaded child pornography from IP addresses assigned to him, then it must be him.

43. SCHWARTZBERG then admitted that he used his cell phone to view child pornography, but that he never uploaded or downloaded anything. SCHWARTZBERG admitted that he may have forwarded a video on a group chat on Kik. SCHWARTZBERG admitted that he knew that child pornography was illegal. SCHWARTZBERG also stated that law enforcement should not find any child pornography on his cell phone.

44. Following the interview SCHWARTZBERG was transported to the West Valley Detention Center.

H. Forensic Examination of SCHWARTZBERG's Cellphone

45. During the search of the SUSPECT RESIDENCE, FPD ICAC seized SCHWARTZBERG's personal cellphone, an iPhone X, SN-FK1W2UWRJCL6. During a forensic examination of the phone, FPD ICAC found a hidden vault application[3] with file folders titled with names of females. One folder, titled "Mxxxxx" contained images and videos a young female who appeared to be between the ages of 13 to 15 years, naked in various positions to display her vagina and/or anal area. At least six videos and 14 images appear to be of the same minor female.

a. As an example, a video file titled "E31C0434-5E35-4718-9BCA-E3FCB677FDCF" is a 13 second video recording, and depicts a pubescent girl about 13-15 years old, in a bathroom, fully nude. After making sure that the camera is correctly angled, she masturbates standing up, facing the camera. Her genitalia and her hand are located at the bottom of the screen but are clearly visible most of the time.

b. An image titled "DC32740-E979-484A-9ACF-4B1E8887A102" depicts the same pubescent girl in a bathroom, fully nude, her right let propped up on the bathroom counter, exposing her genitalia and with at least one finger that appears to be inserted in her genitalia.

46. FPD ICAC also found that the user of the iPhone conducted online searches for "Mxx Mxxxxx" on Google, Instagram and the Whitepages.com. The images and information from the

[3] Based on my training and experience, I know that there are applications which are designed to help users conceal folders on cellular phones.

searches appeared to match the female from the "Mxxxx" hidden vault file.

47. Finally, FPD ICAC also found a Venmo account "xocdrunkx" on SCHWARTZBERG's phone, which was linked to the email account "sagi.schwartzberg@hotmail.com."

I. Interview with Minor Victim 1

48. Detective Moyer searched online for the name "Mxx Xxxxxx" and located a profile on Instagram. An image on the Instagram account had appeared to have been taken in the same room as some of the nude images found on SCHWARTZBERG's phone.

49. An additional online search for "Mxx Xxxxxx Xxxxx" revealed that the victim ("MV 1") attended Agoura High School. Detective Moyer contacted Agoura High School and confirmed the victim attended the school and obtained the contact information for MV 1's parents. On February 19, 2021, Detective Moyer contacted the MV 1's mother via telephone and scheduled an interview for February 22, 2021.

50. In a recorded interview with MV 1 on February 22, 2021, the MV 1 identified herself as being 15 years old. She also identified herself in the images from "Mxxxxx" file.

51. MV 1 reported she was approached online by SnapChat user, "xocdrunkx," using the screen name "Jason," about two years ago. MV 1 accessed her cell phone in front of Detective Moyer to identify the chat thread within Snapchat. She brought up a chat between her and a user with the screen name "Jason D" and a user ID of "xocdrunkx." All of the chats had been

deleted, but MV 1 stated that all of the photos she took were sent to "Jason" ("xocdrunkx") utilizing the chat thread.

52. When asked if she was surprised that her nude images and videos were located on SCHWARTZBERG's phone, MV 1 reported she was not surprised, as she knew "Jason" ("xocdrunkx") had taken a screenshot of her images because Snapchat notified her when anyone screenshots any images she posts. MV 1 stated she did not think anything of it because he had paid her for the images.

53. MV 1 reported she told "Jason" ("xocdrunkx") that she was 13 years old when they first began communicating on Snapchat, and their most recent contact was about one month ago. The chat thread shown to Detective Moyer indicated that that chat thread was last active about five weeks ago.

54. "Jason" ("xocdrunkx") offered to pay her to send him images and videos of herself. MV 1 was paid approximately $600 in Vanilla e-gift cards in 2020 to send "Jason" sexually explicit images and videos of herself. MV 1 estimated that she may have sent "Jason" about 25 images and 2 videos.

55. MV 1 also reported that "Jason" asked her to meet up with him for sex but she never agreed to it. "Jason" also asked her to introduce him to her other friends but MV 1 claimed that she did not introduce him to any of her friends.

56. MV 1 was given a six photo line up, and initially picked out SCHWARTZBERG as "Jason" but then also stated that "Jason" looked like two other men in the photo line up.

57. MV 1 said the Vanilla gift cards were sent to her email account which could be found on her cell phone. MV 1 then pulled up the emails containing the Vanilla e-gift cards and showed them to Detective Moyer. The following is a breakdown of the card numbers, denominations, dates, and messages attached to the gift cards:

Number	**Amount**	**Date**	**Note**
4118 1005 0404 5153 05/2029	$50	05/13/2029 22:33	Mxx
4118 1005 0236 8284 05/2029	$25	5/29/2020 18:12	Mxx from Jason for dinner
4118 1005 0205 6822 06/2029	$25	06/19/2020 16:57	No remitter
4118 1005 0062 0512 07/2029	$50	07/22/2020 14:41	Mxx from J for your trip
4118 1005 0475 1917 08/2029	$50	08/03/2020 16:53	Mxx from Jason
4118 1005 0428 1816 09/2029	$25	12/10/2020 06:15	Mxx Good Luck on your Move
4118 1005 0496 3009 02/2030	$25	10/05/2020 10:29	Mxx for School
4118 1005 0029 1827 02/2030	$25	10/11/2020 20:42	Mxx Enjoy your Vanilla Visa Gift Card

4118 1005 0158 5037 02/2030	$25	11/18/2020 21:26	Mxx surfing stuff
4118 1005 0404 5153 05/2029	$50	05/13/2020 22:33	Mxx
4118 1005 0236 8284 05/2029	%25	05/29/2020 18:12	Mxx from Jason for dinner
4118 1005 0205 6822 06/2029	$25	06/19/2020 16:57	No remitter
4118 1005 0062 0512 07/2029	$50	07/22/2020 14:41	Mxx from J for your trip
4118 1005 0475 1917 08/2029	$50	08/03/2020 16:53	Mxx from Jason
4118 1005 0428 1816 09/2029	$25	12/10/2020 06:15	Mxx Good Luck on Your Move
4118 1005 0496 3009 02/2030	$25	10/05/2020 10:29	Mxx for School
4118 1005 0029 1827 02/2030	$25	10/11/2020 20:42	Mxx Enjoy Your Vanilla Gift Card
4118 1005 0158 5037 02/2030	$25	11/18/2020 21:26	Mxx surfing stuff

58. Two gift cards were also in MV 1's email inbox but had already expired, and Detective Moyer was unable to pull up the gift card numbers and dates for those cards.

59. MV 1 told Detective Moyer that she did not know why "Jason" would write messages like "for school" or "for your

trip." MV 1 confirmed that the gift cards were in exchange for the sexually explicit images of herself that she sent him.

J. Result of Search Warrant Return from Yahoo!

60. During a review of SCHWARTZBERG's cellphone, FPD ICAC had learned that SCHWARTZBERG had an email account, "sagi.schwartzberg@hotmail.com", that had received emails from Venmo for the account with username of "xocdrunkx." Detective Moyer obtained a state search warrant for Yahoo! Email accounts "hoping4achance@yahoo.com" and "xocdrunkx@yahoo.com." During the review of SCHWARTZBERG's phone, FPD ICAC found that "xocdrunkx@yahoo.com" was the email that was linked to SCHWARTZBERG's Apple account on his iPhone.

61. Yahoo! Responded to the search warrant and provided, among others, login data for both email accounts. The email account "hoping4achance@yahoo.com" was accessed on December 9, 2020, from SUSPECT IP 1, which is assigned to SCHWARTZBERG's law office.

62. The email account "xocdrunkx@yahoo.com" was accessed on August 4, 2020, and on October 30, 2020, from SUSPECT IP 1, SCHWARTZBERG's law office. This email account was also accessed from SUSPECT IP 2, which is assigned SCHWARTZBERG's personal residence and SUSPECT RESIDENCE.

K. Identification and Interview of Minor Victim 2

63. FPD ICAC located another minor female ("MV 2")whose images were found on SCHWARTZBERG's phone. MV 2 is currently a 17 year old high school student in Rancho Cucamonga. MV 2's mother brought MV 2 to the Fontana Police Department station for

an interview, at the request of FPD ICAC. MV 2 admitted to sending images of herself on Snapchat. MV 2 readily identified her photos when shown some of the photos and videos of herself from SCHWARTZBERG's phone. MV 2 remembered that she took and sent these photos and videos when she was 16 years old to a Snapchat user "Jason D" with user ID of "xocdrunkx."

64. MV 2 sent "Jason D" videos and photos of herself from March 2020 through December 2020, and received approximately $510 in return. MV 2 never met "Jason D" and only communicated with him via SnapChat. "Jason D" offered to meet up with her and to pay her for sex, but MV 2 never met up with him in person.

65. When "Jason D" would request images and videos from MV 2, he was very specific in instructions, such as, "Can you send me a picture of your pussy or your fingering your pussy." "Jason D" would also request that MV 2 create recordings of herself engaging in sex with another man in certain positions and send the recording to him.

66. MV 2 never told "Jason D" how old she is. A search history on SCHWARTZBERG's phone's search history showed that SCHWARTZBERG had viewed MV 2's Facebook profile at least once.

L. Identification and Interview of Minor Victim 3 and 4

67. FPD ICAC identified two sisters in Minnesota, whose images were also found in the private vault in SCHWARTZBERG's phone, and sought FBI's assistance in interviewing the two sisters (Minor Victim 3 "MV 3" and Minor Victim 4 "MV 4").

68. MV 3 is currently 19 years old and met "xocdrunk" on seeking.com, a dating website. After connecting with MV 3 on seeking.com, "xocdrunk" then found her on Snapchat. "Xocdrunk" would then offer her money in exchange for nude photos of MV 3. MV 3 did send him some photos of herself via Snapchat. MV 3 stated that "xocdrunk" would tell her that her price was too high and that he could get photos from other girls for cheaper and try to get her to provide him with photos of herself for a lower price. MV 3 recalled that images that she sent to "xocdrunk" depicted her breasts, but that "xocdrunk" would ask her to shave her pubic areas for the photos as well.

69. MV 3 identified some of the images of herself found on SCHWARTZBERG's phone and remarked that she wasn't sure whether she was 17 or 18 years old when she sent "xocdrunk" these images but thinks that she was 17 years old based on how skinny she looked in the photos.

70. MV 3 was aware that her younger sister, who is still a minor ("MV 4"), was in contact with "xocdrunk" but could not recall if she had introduced her sister to "xocdrunk" or whether "xocdrunk" had connected with MV 4 on his own. MV 3 denied having been requested to create or send any sexually explicit images of herself and MV 4 together by "xocdrunk." MV 3 was aware that "xocdrunk" was seeking nude photos from MV 4.

71. FBI Minnesota has recently completed an interview with MV 4 but I have not had a chance to review a recording of the interview or a report of the interview.

M. Identification and Interview of Minor Victim 5

72. NCMEC notified FPD ICAC of Cybertip Report 87219116 that it had identified a female, now 18 years old ("MV 5"), who had traded sexually explicit materials when she was 17 years old for money through Venmo, and that one of the buyers was SCHWARTZBERG. Detective Moyer interviewed MV 5 over the phone.

73. MV 5 admitted to Detective Moyer that a couple of years ago around when she was a minor, she provided nude photos of herself to people she had met in a Kik group. MV 5 told Detective Moyer that she had been offered money for photos of herself and would always tell the other person that she was 17 years old. MV 5 stated that she only did it a couple of times in a short period in her life, and doesn't do that anymore.

74. MV 5 told Detective Moyer that her photos would not be easily identifiable because she never showed her face. MV 5 thought that the photos were probably taken in a shower.

VI. REQUEST FOR SEALING

75. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and complaint affidavit. I believe that sealing is necessary because disclosure of complaint affidavit at this time would seriously jeopardize the investigation, as such disclosure may provide an opportunity to destroy evidence, change patterns of behavior, or allow flight from prosecution. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on this

continuing investigation and may severely jeopardize its effectiveness.

VII. CONCLUSION

76. For all the reasons described above, there is probable cause to believe that SCHWARTZBERG violated 18 U.S.C. § 2251(a) (Production of Child Pornography).

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 27th day of April, 2021.

UNITED STATES MAGISTRATE JUDGE