

AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Eastern District of Kentucky

United States of America )

v. )

Mayank M. Patel )

Case No. )

5:23-MJ-5035-MAS )

Defendant(s)

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 Dec. 6, 2017; Jan. 23, 2023 in the county of Fayette in the Eastern District of Kentucky, the defendant(s) violated:

Table with 2 columns: Code Section, Offense Description. Rows include § 18 U.S.C. 2251(a) and § 18 U.S.C. 2252(a)(4)(B) with corresponding offense descriptions.

This criminal complaint is based on these facts:

See attached Affidavit of Special Agent James F. Bugg, which is incorporated and made a part hereof.

Continued on the attached sheet.

/s/ James F. Bugg

Complainant's signature

James F. Bugg, Special Agent

Printed name and title

Transmitted by email and attested to by telephone in accordance with FRCrP 4.1.

Date: 01/27/2023

Handwritten signature of Matthew A. Stinnett

Judge's signature

City and state: Lexington, Kentucky

Matthew A. Stinnett, US Magistrate Judge

Printed name and title

## **AFFIDAVIT**

I, James F. Bugg, a Special Agent (SA) with Homeland Security Investigations (HSI), being duly sworn, depose and state as follows:

### **INTRODUCTION**

1. I have been employed as a Special Agent of the U.S. Department of Homeland Security, Homeland Security Investigations (HSI) for three years and am currently assigned to the Northern Kentucky office.

2. While employed by HSI, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. I am responsible for investigations involving the production, importation, receipt and distribution of child pornography that occur in the Eastern District of Kentucky. I have participated – in all aspects – in investigations involving these offenses. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251 and 18 U.S.C. §§ 2252, I am authorized by law to request an arrest warrant.

3. The facts set forth in this affidavit are based on my own personal knowledge, knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers, my review of documents and computer records related to this investigation, communications with others who have personal knowledge of the events and circumstances described herein, and information gained through my training and experience. This affidavit does not contain every fact known to me with respect to this investigation. Rather, it

contains those facts that I believe to be necessary to establish probable cause for the issuance of the requested criminal complaint.

4. Because this affidavit is being submitted for the limited purpose of securing a criminal complaint and arrest warrant, the affiant has not included each fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause for the listed offenses.

5. For the reasons set out below, there is probable cause to believe that **Mayank M. PATEL**, while in Fayette County, Kentucky, in the Eastern District of Kentucky, committed several offenses involving the sexual exploitation of children, including, but not limited to, employing, using, persuading, inducing, enticing, or coercing any minor to engage in, or to have a minor sexually explicit conduct for the purpose of producing any visual depiction of such conduct.

#### **STATUTORY AUTHORITY**

6. This investigation concerns alleged violations of 18 U.S.C. § 2251(a) and 18 U.S.C. § 2252, relating to material involving the sexual exploitation of minors and a person transporting, distributing, receiving, and possessing material depicting minors engaged in sexually explicit conduct.

a. 18 U.S.C. §2251(a) prohibits a person from employing, using, persuading, inducing, enticing, or coercing any minor to engage in, or to have a minor assist any other person to engage in, or to transport any minor in or affecting interstate or foreign commerce, or in any Territory or Possession of the United States, with the intent that such minor engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for purpose of transmitting a live visual depiction of such conduct if such person knows that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign

commerce or in or affecting interstate or foreign commerce or mailed, or if that visual depiction was produced or transmitted using materials that have been mailed shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

b. 18 U.S.C. §2252(a)(4)(B) prohibits a person from knowingly possessing materials depicting a minor engaged in sexually explicit conduct that has been transported or shipped in interstate commerce or using any means or facility of interstate or foreign commerce, including by computer.

### **BACKGROUND OF CHAT APPLICATION A**

7. This investigation involves a secure chat platform, hereinafter referred to as “Chat Application A.”<sup>1</sup> In review of Chat Application A’s website<sup>2</sup> and other law enforcement resources, I have learned that Chat Application A is a communications-based platform available on the internet to users worldwide. Chat Application A’s services include instant messaging, voice calls, video calls, and file sharing capabilities. Chat Application A allows users to have personal, one-on-one chats, or to have larger scale group chats with other Chat Application A users.

All Chat Application A chats are protected by end-to-end encryption, meaning that only the sender and receiver(s) of a chat have access to the content, and nothing is stored on any servers once delivered.

8. To access Chat Application A, a user must create an account, which requires him or her to provide a cellular phone number. The account cellular phone number is sent a verification text message with a verification key code that must be entered in the application in order to activate

---

<sup>1</sup> Law enforcement knows the actual name of Chat Application A. However, the investigation into users of Chat Application A remains ongoing, and public disclosure of Chat Application A’s actual name potentially would alert its members to the investigation and cause members to flee or destroy evidence. Accordingly, to preserve the confidentiality and integrity of the ongoing investigation, the actual name and other identifying details of Chat Application A remain undisclosed in this affidavit.

<sup>2</sup> I know that Chat Application A updates its website content and informational blog posts often, and the information set forth here is derived in part from information obtained from Chat Application A’s website as of the date that this affidavit was drafted.

the account. A user also is asked to provide a full name, birthdate, and email. The full name field, which becomes the user's display name in the application, is the only field required to continue into the application and can be any name the user chooses to enter. Upon opening Chat Application A, both the user's verified phone number and display name are visible on the right side of the messaging board.

9. Chat Application A has a "My Notes" feature, which is a dedicated space within a user's chat list. This space allows a user to save messages, images, and videos.

10. Chat Application A also provides for three different formats of large-scale chatting: groups, communities, and channels.<sup>3</sup>

11. According to Chat Application A's website, a group is a private chat with multiple people. It generally is intended to be used by people who know each other and only allows up to 250 people to join. According to Chat Application A's website, groups are not subject to content restrictions and have few moderation features. Groups are not available to the general public and searching for them by name within Chat Application A will not yield any results. Participants<sup>4</sup> gain access to groups by clicking an invitation link or being added directly by other Chat Application A users. Any user can select and add any of their contacts or non-contacts to a Chat Application A group, and unless certain privacy settings have been activated by the user to be added,<sup>5</sup> he/she automatically will be added to that group. A participant in a group can leave the group at any time. For as long as a user remains a participant in a group, the user will be able to

---

<sup>3</sup> For the purpose of this affidavit, only Chat Application A groups and communities will be discussed.

<sup>4</sup> Law enforcement officers that have used Chat Application A in an undercover role have learned that in groups on Chat Application A, users are referred to as "participants." In communities, users are referred to as "members."

<sup>5</sup> Chat Application A has a privacy setting that allows a user to prevent noncontacts from automatically adding that user to a group.

access all chat history and content sent since the date that the user joined that group. The full list of participants in a group is displayed on the side of the group, and also in the group's "Info" screen. The total number of participants, which participants are admins, and all participants' display names and verified phone numbers are visible to all group participants in the group's info screen. Groups also can have a group icon and group name, which anyone in the group has the ability to change.

12. Additionally, Chat Application A has large-scale chats known as communities. Communities are different from groups in several ways, including that they are much larger and usually are made up of people who do not know one another. According to Chat Application A's website, communities can have unlimited members.<sup>6</sup> In addition to admins, communities also contain a "superadmin," who was the creator of the community. Only the superadmin can change the name, icon, and description of the community. There are two ways that a member can be added to a community: by receiving and clicking on a link invitation or being added directly by a previously saved contact. Unlike groups, community members cannot add a new user unless they already have that user saved as a contact. Also, unlike groups, the superadmin of a community has complete control over who can access the community invitation link. The superadmin can disable link invites if they are forwarded to unintended recipients and can turn off members' ability to share the invite link. Communities afford additional privacy settings that groups do not, such as preventing members from viewing other members' verified phone numbers.<sup>7</sup> Unlike groups, communities are private by default, though they can be made public. To make a community public,

---

<sup>6</sup> As mentioned previously, law enforcement officers that have used Chat Application A in an undercover capacity have learned that in communities, users are referred to as members.

<sup>7</sup> Law enforcement officers that have used Chat Application A in an undercover capacity have learned that a community member's phone number still will be visible to other community members if both members are also participants in at least one of the same groups on Chat Application A.

a superadmin must contact Chat Application A. A member of a community can leave the community at any time. For as long as the member remains in the community, the member can view the community's entire chat history and content, starting from the date that the community was established.

### PROBABLE CAUSE

13. The investigation of **Mayank M. PATEL** began because law enforcement observed that **Mayank M. PATEL** was a member of private communities and at least one private group for at least three (3) months and was a member of additional private groups for an unknown length of time, and these groups and communities were involved in the distribution of child pornography within Chat Application A.

14. HSI Northern Kentucky obtained access to and assumed an account on Chat Application A ("Assumed Account 1"). Through Assumed Account 1, HSI Northern Kentucky gained access to 81 community and/or group chats involved in the distribution of child pornography within Chat Application A.

15. One community in which Assumed Account 1 was present, hereinafter "Community A" also had member with a certain username<sup>8</sup> and the verified phone number (XXX) XXX-8414 (hereinafter the "8414 ACCOUNT").<sup>9</sup> Community A is private and a search for their names on Chat Application A will not yield any results. The 8414 ACCOUNT was a member of Community A when then contents of the communities' chats were viewed by HSI Northern

---

<sup>8</sup> The full username is known to law enforcement but redacted here to preserve the confidentiality and integrity of the ongoing investigation.

<sup>9</sup> As explained above, *see supra* n.7, though communities do not display all members' verified phone numbers like groups do, communities will show a community member the verified phone numbers of other community members who also are participants in at least one of the same Chat Application A groups as the first community member. In this case, the verified phone number of the 8414 ACCOUNT was visible to Assumed Account 1 because both community members also were participants in at least one of the same groups, as is described below.

Kentucky for evidentiary purposes on January 23, 2023. As a member of Community A on January 23, 2022, the 8414 ACCOUNT had the ability to view and download all files that previously had been distributed within each community from that community's date of inception through January 23, 2023.

16. On January 23, 2023, HSI Northern Kentucky Special Agents viewed Community A on Chat Application A to see an approximately thirty-seven (37) second video with an approximately ten to twelve-year-old, Caucasian male, remove his clothing, exposing his naked, erect penis and begin masturbating. The video was uploaded to Community A on December 1, 2022. Mayank M. PATEL was a member of Community A at the time of upload on December 1, 2022 and was currently a member of Community A at the time Special Agents viewed the image on January 23, 2023.

17. On January 23, 2023, HSI SA Borders and Kentucky State Police (KSP) Detective Gatson proceeded to 3300 Montavesta Drive, Apt. 5202, Lexington, KY 40502 and conducted a knock and talk with **Mayank M. PATEL**.

18. **Mayank M. PATEL** agreed to speak with investigators privately in Detective Gatson's KSP vehicle. It was made clear to **Mayank M. PATEL** that he was not under arrest and was free to leave at any time. **Mayank M. PATEL** read a statement of his rights, which he agreed to waive.

19. **Mayank M. PATEL** also agreed to a consent search of his devices, an Apple iPhone 12 Pro, IMEI 354523335k714443, SN# A2341 and Apple MacBook Pro M1 Model #A2338, SN# C02DMPPRQ05D.

20. **Mayank M. PATEL** admitted to SA Borders and Detective Gatson that the 8414 ACCOUNT did in fact belong to him. **Mayank M. PATEL** admitted to being a part of at least



thirty (30) Community's that specifically existed to receive and distribute child sexual abuse material. **Mayank M. PATEL** admitted that he possessed child sexual abuse material on his Apple iPhone 12 Pro, IMEI 354523335k714443, SN# A2341 and his Apple MacBook Pro M1 Model #A2338, SN# C02DMPPRQ05D. **Mayank M. PATEL** admitted to viewing hardcore and violent child sexual abuse material that included serious bodily harm to infants. **Mayank M. PATEL** admitted that he last logged on to Chat Application A the morning of January 23, 2023, and that he usually logs on at least once a day. **Mayank M. PATEL** admitted to utilizing other chat applications to access child sexual abuse material.

21. **Mayank M. PATEL** admitted that he took his Apple iPhone 12 Pro, IMEI 354523335k714443, SN# A2341 with him on a recent trip to India and that he accessed Chat Application A, and that he brought that phone back with him to the United States when he returned.

22. **Mayank M. PATEL** also disclosed to investigators that he had committed sexual acts with his minor neighbor, Victim 1, who was approximately 7 to 8 years of age at the time. These sexual acts included having the child place her mouth on **Mayank M. Patel's** erect penis. **Mayank M. PATEL** stated he recorded this act, which was stored logically on both of his devices and backed up on his iCloud account. In addition to recording sexual acts with Victim 1, **Mayank M. PATEL** disclosed he also took pictures of Victim 1's vagina and breasts on two (2) different occasions.

22. During the consent search of **Mayank M. PATEL's** iPhone and MacBook, forensic investigators were able to locate the video depicting Victim 1 that **Mayank M. PATEL** had previously described. The video is listed as IMG\_0037.mov. During the video, Victim 1's face is visible, and **Mayank M. PATEL's** erect penis is visible and is in Victim 1's mouth. Victim 1 can be heard saying "Don't pee in my mouth." The video is twenty-two seconds in length and

shows a creation date of December 6, 2017. Based on the creation date, at the time of the video Victim 1 would have been seven years old.

23. Your affiant knows that Apple iPhones and Apple MacBooks are not manufactured in the Commonwealth of Kentucky. He also knows that the term “means or facility of interstate commerce” includes the internet or telephones.

### CONCLUSION

24. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that while in the Eastern District of Kentucky, Fayette County, Kentucky, **Mayank M. PATEL** engaged in the following:


a. On or about December 6, 2017, **Mayank M. PATEL** knowingly used, persuaded, induced, enticed, and coerced a minor to engage in sexually explicit conduct for the purpose of producing visual depictions of such conduct, knowing and having reason to know that such visual depiction would be transported and transmitted using any means or facility of interstate commerce, or that visual depiction was produced or transmitted using materials that had been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, in violation of 18 U.S.C. §§ 2251(a).

b. On or about January 23, 2023, **Mayank M. PATEL** possessed materials depicting a minor engaged in sexually explicit conduct that had been transported or shipped in interstate commerce or using any means or facility of interstate or foreign commerce, including by computer.

/s/ James F. Bugg

James F. Bugg  
Special Agent  
Homeland Security Investigations

Sworn to/attested to by the affiant in accordance with the requirements of Fed. R. Crim. P. 4.1  
by telephone or other reliable electronic means this 27 day of January 2023.

  
Matthew A. Stirmett  
Matthew A. Stirmett  
United States Magistrate Judge