

JACQUELINE FORD
MANMEET DHINDSA
ALEJANDRO ROSENBERG
(Each appearing pursuant to DUCivR 83-1.1(b)(1))
Federal Trade Commission
600 Pennsylvania Ave., N.W., CC-6316
Washington, D.C. 20580
Telephone: (202) 326-2844
jford1@ftc.gov
mdhindsa@ftc.gov
arosenberg@ftc.gov
Attorneys for Plaintiff
FEDERAL TRADE COMMISSION

DOUGLAS CRAPO (14620)
STEVENSON SMITH (18546)
CARINA WELLS (19112)
Utah Attorney General's Office
160 East 300 South, Fifth Floor
Salt Lake City, UT 84114
Telephone: (801) 366-0310
crapo@agutah.gov
scsmith@agutah.gov
cwells@agutah.gov
Attorneys for Plaintiff
UTAH DIVISION OF CONSUMER PROTECTION

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF UTAH**

FEDERAL TRADE COMMISSION, and
UTAH DIVISION OF CONSUMER
PROTECTION,

Plaintiffs,

v.

AYLO GROUP LTD., a Cypriot corporation,

DONORMASS LIMITED, a Cypriot
corporation,

AYLO FREESITES LTD., a Cypriot
corporation,

AYLO PREMIUM LTD., a Cypriot
corporation,

AYLO TECHNOLOGIES LTD., a Cypriot
corporation,

9279-2738 QUEBEC INC., a Canadian
corporation,

9219-1568 QUEBEC INC., a Canadian
corporation,

AYLO HOLDINGS USA CORP., a Delaware
corporation,

AYLO BILLING US CORP., a Delaware
corporation,

**COMPLAINT FOR PERMANENT
INJUNCTION, MONETARY
JUDGMENT, AND OTHER RELIEF¹**

Case No.

¹ CONTENT WARNING: This Complaint contains references to, and descriptions of, various sensitive content, including pornographic content, sexually explicit content involving minors, violence, kidnapping, sexual assault, and other non-consensual acts.

TOQON, LLC, a Delaware limited liability company,

AYLO GLOBAL ENTERTAINMENT INC., a Delaware corporation,

AYLO USA INCORPORATED, a Delaware corporation,

FTSA, LLC, a Delaware limited liability company, and

AYLO BILLING LIMITED, an Irish corporation,

Defendants.

Plaintiffs, the Federal Trade Commission (“FTC”) and the Utah Division of Consumer Protection (“Division”), for their Complaint allege:

1. The FTC brings this action for Defendants’ violations of Section 5(a) of the Federal Trade Commission Act (“FTC Act”), 15 U.S.C. § 45(a). For these violations, the FTC seeks relief, including a permanent injunction and other relief, pursuant to Section 13(b) of the FTC Act, 15 U.S.C. § 53(b).

2. The Division brings this action for Defendants’ violations of the Utah Consumer Sales Practices Act (“UCSPA”), Utah Code § 13-11-1 *et seq.* For these violations, the Division seeks relief, including injunctive relief and civil penalties and fines, under the UCSPA, Utah Code § 13-11-17(1).

SUMMARY OF CASE

3. Defendants own and operate Pornhub.com and some of the other largest and most popular pornography websites in the world. In 2021, these sites collectively saw over 800 million

monthly visits from U.S. consumers, including users from Utah. Since 2012, Defendants have distributed tens of thousands of videos and photos featuring child sexual abuse material (“CSAM”) and non-consensual material (“NCM”)—content produced and/or distributed without the consent of someone featured therein, such as revenge porn, spy camera videos, and rape videos. Defendants’ publication of such content on their websites has resulted in a member of Defendants’ Compliance team describing Pornhub.com as “a goldmine” for “rape content.” And consumers have viewed and downloaded (and then further distributed) this content millions of times, often not knowing it was CSAM or NCM.

4. Defendants coordinate with professional studios to create content, and Defendants publish this content through channels on their websites. Some of this content had titles suggesting that the content was CSAM or NCM, such as “brutal castings,” “helpless boys,” “helpless teens,” “internet creeper,” “shower spy cameras,” and “shamed sluts.” Internally, Defendants have recognized that these channels routinely contain “Non-consent,” “Non-consensual sexual violence,” “Revenge content,” “Kidnapping,” “Violence,” and “Hidden Camera.”

5. For example, Defendants published a professional studio’s content through a channel on Pornhub.com titled “boys for sale,” which was marketed as an “underground secret society of men who buy and sell boy slaves on the black market” and “once groomed by the society they are prepared for a life of servicing the men who buy and use and breed their young vi[r]ginal bodies.” Defendants monetized these videos for years, even though Defendants recognized that the videos featured “Slavery” and raised “underage concerns.”

6. Defendants have also specifically encouraged users to upload content to their websites using tags that suggest the content contains CSAM and NCM. Defendants then offered this illegal and damaging content to consumers in playlists with titles such as “less than 18,” “the best collection of young boys,” and “under-age,” which they promoted on their websites.

7. Defendants have engaged in this conduct for years despite intense public scrutiny and Defendants’ own recognition that most consumers do not want to be exposed to such content. Rather than change their practices, Defendants have instead engaged in a public campaign of deception, repeatedly telling consumers—in the press, in blog posts, and in policy statements—that they take serious steps to keep CSAM and NCM off their websites. In other words, Defendants simultaneously distributed CSAM and NCM and engaged in a public relations campaign to deceive consumers into believing that their websites are free from that very same content.

8. Specifically, beginning in 2018, Defendants falsely promised to quickly review and remove website content that consumers flagged as being illegal or in violation of Defendants’ terms of service. In reality, Defendants ignored hundreds of thousands of these flags—thousands of which flagged content as CSAM and NCM—for years, allowing the content to stay live. When Defendants did finally review these flagged videos in 2020 and 2021, they removed thousands of them as CSAM and NCM.

9. Defendants have also falsely promised to (1) ban users who uploaded CSAM to their websites, (2) maintain documentation required under 18 U.S.C. § 2257 establishing the age and identity of certain performers in Defendants’ subscription-based pornographic content, (3) prevent CSAM from being re-uploaded to their websites, (4) review all content to ensure it does

not contain CSAM or NCM before it goes live on the Defendants' websites, and (5) keep CSAM and NCM off their websites. Defendants have made all of these deceptive statements to lure consumers to their websites on the promise that they did not contain CSAM or NCM.

10. It was only in 2020, when Defendants' credit card processors began threatening Defendants with massive fines and the permanent termination of their relationship, that Defendants' Compliance team began attempting to police CSAM and NCM on their websites. But, even then, Defendants routinely ignored or overruled such efforts, maintaining tens of thousands of CSAM and NCM videos and photos on their websites.

11. Defendants also engage in deceptive practices in connection with their collection, use, and security of consumers' personal information. Prior to December 2020, Defendants required members of their Model Program ("Models") to submit verification images (a photo that includes, among other things, "most" of the Model's face) prior to uploading any content eligible for payment. Defendants told Models that the images would be stored securely and kept "totally private." Beginning in December 2020, Defendants have required consumers to verify their identities—through the submission of governmental identification to a separate vendor—before they can upload pornographic content to the Defendants' websites. Defendants tell consumers that this documentation, including driver's licenses, Social Security numbers, and/or passports, will be collected and securely stored by a separate vendor. In truth, that vendor passes the documentation along to Defendants. But Defendants fail to secure the information, including the verification images, and allow their employees to email the documents to one another freely.

JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331, 1337(a), and 1345.

13. This Court has supplemental jurisdiction over the Division's claims under 28 U.S.C. § 1367.

14. Venue is proper in this District under 28 U.S.C. § 1391(b)(3), (c)(2) and (c)(3), and 15 U.S.C. § 53(b).

PLAINTIFFS

15. The FTC is an agency of the United States Government created by the FTC Act, which authorizes the FTC to commence this district court civil action by its own attorneys. 15 U.S.C. §§ 41–58. The FTC enforces Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), which prohibits unfair or deceptive acts or practices in or affecting commerce.

16. The Division is an administrative agency of the Department of Commerce, State of Utah. Utah Code § 13-2-1(1). The Division administers and enforces the UCSPA, which prohibits deceptive or unconscionable acts or practices in connection with consumer transactions.

DEFENDANTS

17. Defendant AYLO Group Ltd. (formerly known as MG CY Holdings Ltd.) is a Cypriot corporation with its principal office or place of business at Block 1, 195-197 Old Nicosia-Limassol Road, Dali Industrial Zone 2540, Cyprus. Defendant AYLO Group Ltd. transacts or has transacted business in this District, Utah, and throughout the United States. At all times relevant to this Complaint, acting alone or in concert with others, Defendant AYLO Group Ltd.

has advertised, marketed, distributed, or sold pornographic content to consumers throughout the United States.

18. Defendant Donormass Limited is a Cypriot corporation with its principal office or place of business at Block 1, 195-197 Old Nicosia-Limassol Road, Dali Industrial Zone 2540, Cyprus. Defendant Donormass Limited transacts or has transacted business in this District, Utah, and throughout the United States. At all times relevant to this Complaint, acting alone or in concert with others, Defendant Donormass Limited has advertised, marketed, distributed, or sold pornographic content to consumers throughout the United States.

19. Defendant AYLO Freesites Ltd. (formerly known as MG Freesites Ltd.), is a Cypriot corporation with its principal office or place of business at Block 1, 195-197 Old Nicosia-Limassol Road, Dali Industrial Zone 2540, Cyprus. Defendant AYLO Freesites Ltd. transacts or has transacted business in this District, Utah, and throughout the United States. At all times relevant to this Complaint, acting alone or in concert with others, Defendant AYLO Freesites Ltd. has advertised, marketed, distributed, or sold pornographic content to consumers throughout the United States.

20. Defendant AYLO Premium Ltd. (formerly known as MG Premium Ltd.) is a Cypriot corporation with its principal office or place of business at Block 1, 195-197 Old Nicosia-Limassol Road, Dali Industrial Zone 2540, Cyprus. Defendant AYLO Premium Ltd. transacts or has transacted business in this District, Utah, and throughout the United States. At all times relevant to this Complaint, acting alone or in concert with others, Defendant AYLO Premium Ltd. has advertised, marketed, distributed, or sold pornographic content to consumers throughout the United States.

21. Defendant AYLO Technologies Ltd. (formerly known as MG Technologies Ltd.) is a Cypriot corporation with its principal office or place of business at Block 1, 195-197 Old Nicosia-Limassol Road, Dali Industrial Zone 2540, Cyprus. Defendant AYLO Technologies Ltd. transacts or has transacted business in this District, Utah, and throughout the United States. At all times relevant to this Complaint, acting alone or in concert with others, Defendant AYLO Technologies Ltd. has advertised, marketed, distributed, or sold pornographic content to consumers throughout the United States.

22. Defendant 9279-2738 Quebec Inc. is a Canadian corporation with its principal office or place of business at 777 Decarie Boulevard, Suite 300, Montreal, Quebec, H4P 2H2, Canada. Defendant 9279-2738 Quebec Inc. transacts or has transacted business in this District, Utah, and throughout the United States. At all times relevant to this Complaint, acting alone or in concert with others, Defendant 9279-2738 Quebec Inc. has advertised, marketed, distributed, or sold pornographic content to consumers throughout the United States.

23. Defendant 9219-1568 Quebec Inc. is a Canadian corporation with its principal office or place of business at 777 Decarie Boulevard, Suite 300, Montreal, Quebec, H4P 2H2, Canada. Defendant 9219-1568 Quebec Inc. transacts or has transacted business in this District, Utah, and throughout the United States. At all times relevant to this Complaint, acting alone or in concert with others, Defendant 9219-1568 Quebec Inc. has advertised, marketed, distributed, or sold pornographic content to consumers throughout the United States.

24. Defendant AYLO Holdings USA Corp. (formerly known as MG Holdings USA Corp.) is a Delaware corporation with its principal office or place of business at 21800 Oxnard Street, Suite 150, Woodland Hills, California 91367. Defendant AYLO Holdings USA Corp. transacts

or has transacted business in this District, Utah, and throughout the United States. At all times relevant to this Complaint, acting alone or in concert with others, Defendant AYLO Holdings USA Corp. has advertised, marketed, distributed, or sold pornographic content to consumers throughout the United States.

25. Defendant AYLO Billing US Corp. (formerly known as MG Billing US Corp.) is a Delaware corporation with its principal office or place of business at 21800 Oxnard Street, Suite 150, Woodland Hills, California 91367. Defendant AYLO Billing US Corp. transacts or has transacted business in this District, Utah, and throughout the United States. At all times relevant to this Complaint, acting alone or in concert with others, Defendant AYLO Billing US Corp. has advertised, marketed, distributed, or sold pornographic content to consumers throughout the United States.

26. Defendant Toqon, LLC is a Delaware limited liability company with its principal office or place of business at 21800 Oxnard Street, Suite 150, Woodland Hills, California 91367. Defendant Toqon, LLC transacts or has transacted business in this District, Utah, and throughout the United States. At all times relevant to this Complaint, acting alone or in concert with others, Defendant Toqon, LLC has advertised, marketed, distributed, or sold pornographic content to consumers throughout the United States.

27. Defendant AYLO Global Entertainment (formerly known as MG Global Entertainment Inc.) is a Delaware corporation with its principal office or place of business at 21800 Oxnard Street, Suite 150, Woodland Hills, California 91367. Defendant AYLO Global Entertainment Inc. transacts or has transacted business in this District, Utah, and throughout the United States. At all times relevant to this Complaint, acting alone or in concert with others, Defendant AYLO

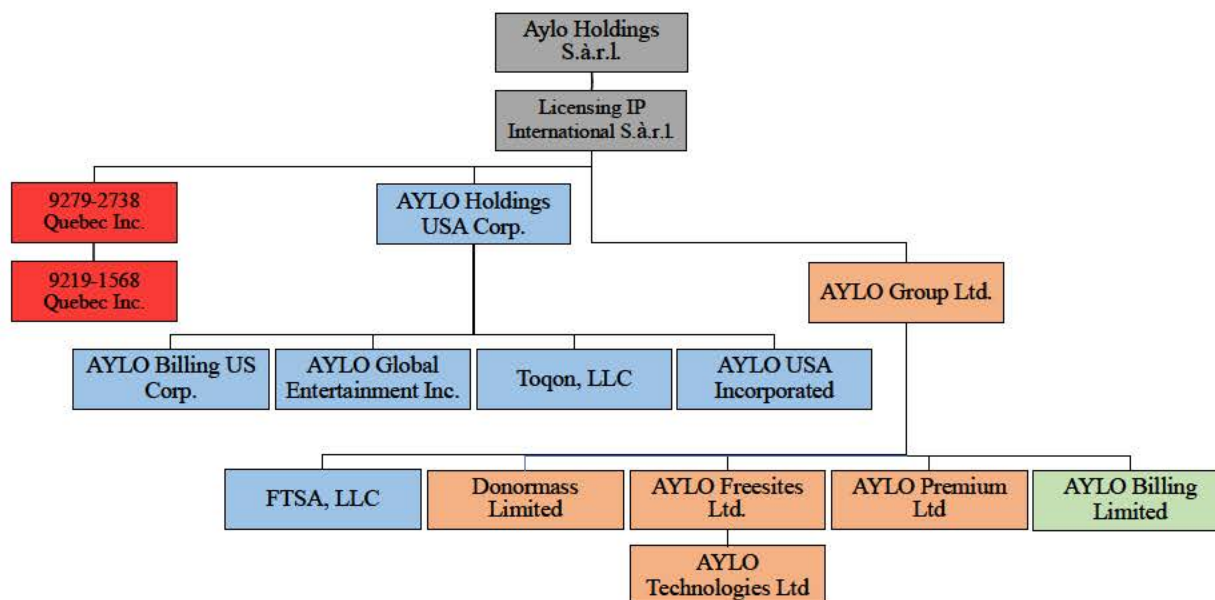
Global Entertainment Inc. has advertised, marketed, distributed, or sold pornographic content to consumers throughout the United States.

28. Defendant AYLO USA Incorporated (formerly known as MindGeek USA Incorporated) is a Delaware corporation with its principal office or place of business at 21800 Oxnard Street, Suite 150, Woodland Hills, California 91367. Defendant AYLO USA Incorporated transacts or has transacted business in this District, Utah, and throughout the United States. At all times relevant to this Complaint, acting alone or in concert with others, Defendant AYLO USA Incorporated has advertised, marketed, distributed, or sold pornographic content to consumers throughout the United States.

29. Defendant FTSA, LLC, is a Delaware limited liability company with its principal place of business at 21800 Oxnard Street, Suite 150, Woodland Hills, California 91367. Defendant FTSA, LLC transacts or has transacted business in this District, Utah, and throughout the United States. At all times relevant to this Complaint, acting alone or in concert with others, Defendant FTSA, LLC has advertised, marketed, distributed, or sold pornographic content to consumers throughout the United States.

30. Defendant AYLO Billing Limited (formerly known as MG Billing Limited) is an Irish corporation with its principal place of business at 24-26 City Quay, Dublin 2, Ireland. Defendant AYLO Billing Limited transacts or has transacted business in this District, Utah, and throughout the United States. At all times relevant to this Complaint, acting alone or in concert with others, Defendant AYLO Billing Limited has advertised, marketed, distributed, or sold pornographic content to consumers throughout the United States.

31. Defendants' corporate organizational structure is set forth in the image below (with the Cyprus entities in orange, the Canadian entities in red, the U.S. entities in blue, and AYLO Billing Limited in green), indicating common ownership under Aylo Holdings S.à.r.l.:



COMMON ENTERPRISE

32. Defendants have operated as a common enterprise while engaging in the unlawful acts and practices alleged below. In particular, Defendants work jointly to carry out the business practices described below, namely owning and operating their adult-video websites, through an interrelated network of companies that have common control and ownership; shared officers, managers, employees, business functions, office space, and email systems; unified advertising; and commingled funds. Because Defendants have operated as a common enterprise, each of them is liable for the acts and practices alleged below.

COMMERCE

33. At all times relevant to this Complaint, Defendants have maintained a substantial course of trade in or affecting commerce, as “commerce” is defined in Section 4 of the FTC Act, 15 U.S.C. § 44.

DEFENDANTS’ BUSINESS ACTIVITIES

The Services and Content Production

34. Defendants own and operate over 100 pornographic photo and video-streaming websites, all of which are available around the world, including in the United States. Defendants’ websites fall into two categories: free, ad-based sites (the “Tube Sites”) and subscription-based sites (the “Pay Sites”).

35. Defendants work to attract as much web traffic to these sites as possible to maximize advertising and subscriber revenue. Defendants draw this traffic, and maintain first position in the market, by offering an ever-growing supply of pornographic content. Defendants’ flagship Tube Site, Pornhub.com, is one of the largest and most-visited websites on the internet. Collectively, as of 2021, Defendants’ websites saw over 800 million monthly visits by consumers in the United States alone. As of 2020, the Tube Sites had over 8 million users in the United States, including users from Utah. As of 2020, the Pay Sites had over 1.3 million paying subscribers, including subscribers from Utah.

36. Defendants earned over \$350 million in subscription revenue in 2020, with over \$190 million of that figure coming from U.S. consumers. Defendants earned over \$250 million in subscription revenue in 2021, with over \$100 million of that figure coming from U.S. consumers.

The Tube Sites

37. The Tube Sites include Pornhub.com (“Pornhub”), Youporn.com (“YouPorn”), Redtube.com (“RedTube”), Tube8.com (“Tube8”), Xtube.com (“XTube”), Thumbzilla.com (“Thumbzilla”), Spankwire.com (“SpankWire”), Mofosex.com (“MofoSex”), Keezmovies.com (“KeezMovies”), and Extremetube.com (“ExtremeTube”). Defendant AYLO Freesites Ltd., which operates the Tube Sites, does business under each of these names.

38. To attract web traffic, Defendants continually add and draw as much new content to the Tube Sites as possible. Over 5.5 million videos were added to the Tube Sites in 2018. Over 7.5 million videos were added to the Tube Sites in 2019. And, in 2020, over 12 million videos were added to the Tube Sites.

39. Until December 2020, videos and photos were added to the Tube Sites in four ways:

- a. Defendants selected and purchased videos, which they directly uploaded to the Tube Sites;
- b. As detailed below, Defendants coordinated with professional studios (“Content Partners”), to create content for designated channels on the Tube Sites;
- c. Defendants recruited Models, who uploaded content to the Tube Sites; and
- d. As detailed below, Defendants solicited users to upload content to the Tube Sites, often specifically encouraging that these users upload “teen” content, which was often CSAM and/or NCM.

40. Regardless of the source, Defendants optimize or select each video’s title, tags, and categories, as well as choose the best thumbnails to make the video more attractive to consumers.

41. Until December 2020, any individual could upload pornographic videos and photos to the Tube Sites without any verification by Defendants as to the identity, age, or consent of the uploader or any individual featured in the content. Furthermore, until December 2020, Defendants made all content on the Tube Sites available for free viewing and download. As a result, consumers uploaded millions of videos and photos to the Tube Sites each year, including tens of thousands of CSAM and NCM videos and photos. Consumers then viewed and downloaded these videos and photos, including the CSAM and NCM videos and photos, from the Tube Sites millions of times. Consumers regularly downloaded this content, including the CSAM and NCM videos and photos (often not knowing it was CSAM or NCM), often re-uploading it to other websites or otherwise disseminating the material.

42. In December 2020, in response to an Op-Ed in The New York Times alleging that Pornhub was full of thousands of CSAM and NCM videos, Defendants restricted uploads to Content Providers and Models, who were required to verify their identities and ages through the submission of government-issued identification. At the same time, Defendants also removed the ability for consumers to download most content from their websites. As a result, consumers can now view, but not download, content on the Tube Sites.

The Pay Sites

43. The Pay Sites include 8thstreetlatinas.com, Adult.com, Babes.com, Babesnetwork.com, Babespremium.com, Bigdicksatschool.com, Bignaturals.com, Bigstr.com, Blackgfs.com, Blackmaleme.com, Brazzers.com, Brazzersenespanol.com, Brazzersnetwork.com, Brazzersplus.com, Brazzerspromo.com, Bromo.com, Bustedbabysitters.com, Captainstabbin.com, Crazyasiangfs.com, Crazycollegegfs.com, Cumfiesta.com,

Czechhunter.com, Daredorm.com, Debt dandy.com, Dickdorm.com, Digitalplayground.com, Digitalplaygroundpremium.com, Dirtyscout.com, Dontbreakme.com, Dontbreakmepremium.com, Drillmyhole.com, Elitexxx.com, Erito.com, Eritopremium.com, Extremetubepremium.com, Gf leaks.com, Godsofmen.com, Happytugs.com, Hardcorekings.com, Hentaipros.com, Hentaiprospremium.com, Iknowthatgirl.com, Iknowthatgirlpremium.com, Inthevip.com, Jizzorgy.com, Keezmoviespremium.com, Latinasextapes.com, Letstryanal.com, Lezdombliss.com, Lilhumpers.com, Lookathernow.com, Maleaccess.com, Men.com, Menofuk.com, Mikesapartment.com, Milfhunter.com, Modelhub.com, Mofos.com, Mofosexpremium.com, Mofosnetwork.com, Mofospremium.com, Momsbangteens.com, Momslickteens.com, Moneytalks.com, Mydirtyclub.com, Mydirtyhobby.com, Mydirtyhobby.de, Nutaku.com, Nutaku.net, Pervsonpatrol.com, Pornhubpremium.com, Privatamateure.com, Privat-Amateure.com, Privateamateur.com, Publicpickups.com, Realitydudes.com, Realitydudesnetwork.com, Realitykings.com, Redtubeplatinum.com, Redtubepremium.com, Rk.com, Roundandbrown.com, Seancody.com, Shesafreak.com, Sneakysex.com, Spankwirepremium.com, Squirted.com, Str8chaser.com, Str8togay.com, Teenpinkvideos.com, Teenslovehugecocks.com, Thegayoffice.com, Toptobottom.com, Trannysurprise.com, Transangels.com, Transangelspremium.com, Transharder.com, Trueamateurs.com, Trueamateurspremium.com, Tube8vip.com, Twistedfamilies.com, Twistys.com, Twistysnetwork.com, Twistyspremium.com, Welivetogether.com, Whengirlsplaypremium.com, Whynotbi.com, and Youpornpremium.com.

44. Defendants co-create all of the videos and photos on the Pay Sites with a number of vendors; in fact, Defendants describe themselves as a “secondary producer” of this content. As

explained by Defendants' Chief Executive Officer in a 2019 interview for a law review article, Defendants contract with these vendors to produce approximately 400 pornographic videos each month for the Pay Sites, at a price of \$5,000 to \$8,000 per video. Kal Raustiala & Christopher Jon Sprigman, *The Second Digital Disruption: Streaming and the Dawn of Data-Driven Creativity*, 94 N.Y.U. L. Rev. 1555, 1591 (2019). He further explained that Defendants utilize the data from the millions of views of other videos on their websites to write the scripts for these videos, giving the vendors detailed dialogue, sex acts, and camera angles which must be included in the videos. Defendants' detailed script instructions state, for example, that a performer "lies on her stomach and looks over her shoulder at the camera" and then gets up and "struts" toward the camera. In some instances, Defendants even specify the furniture and carpet styles to use in scenes. Defendants own or license all of the content on the Pay Sites.

Corporate Structure

45. Defendants function as a common enterprise, acting jointly to operate their aforementioned pornographic websites. Specifically, Defendants are an interrelated network of entities that have common ownership, officers, managers, employees, business functions, and commingled funds.

46. Defendants are all under the common control of one Chief Executive Officer, Chief Operating Officer, Chief Product Officer, Chief Legal Officer, and Chief Financial Officer. These individuals oversee and serve as the decisionmakers for all Defendants. Notably, the individual who served as Defendants' Chief Executive Officer from 2010 to 2022 also served as President and director of Defendants MG Billing US Corp. (now known as AYLO Billing US Corp.), MG Global Entertainment Inc. (now known as AYLO Global Entertainment Inc.), MG

Holdings USA Corp. (now known as AYLO Holdings USA Corp.), and MindGeek USA Incorporated (now known as AYLO USA Incorporated) from at least 2018 to February 2020.

And the individual who served as Defendants' Chief Operating Officer from 2010 to 2022 also served as an officer or director of these same American companies during the same time frame.

47. As of July 2021, Defendants shared over 1,600 employees worldwide, including over two dozen in the United States. Defendants publicly represent, and the employees themselves represent, that they are all employed by "MindGeek" (and now "Aylo," Defendants' assumed name as of August 2023). In addition, Defendants' employees utilize a shared email system, with "@mindgeek.com" ("@aylo.com" as of August 2023) email addresses.

48. Defendants share office space on a regional basis (AYLO Billing Limited has its own offices in Ireland):

- a. Defendants AYLO Group Holdings Ltd., Donormass Ltd., AYLO Freesites Ltd., AYLO Technologies Ltd., and AYLO Premium Ltd. (collectively, the "Cyprus Companies") share offices at Block 1, 195-197 Old Nicosia-Limassol Road, Dali Industrial Zone 2540, Cyprus.
- b. Defendants 9279-2738 Quebec Inc. and 9219-1568 Quebec Inc. (collectively, the "Canadian Companies") share offices at 777 Decarie Boulevard, Suite 300, Montreal, Quebec, H4P 2H2, Canada.
- c. Defendants AYLO Holdings USA Corp.; AYLO Billing US Corp.; AYLO Global Entertainment Inc.; Toqon, LLC; FTSA, LLC; and AYLO USA Incorporated (collectively, the "U.S. Companies") share offices at 21800 Oxnard Street, Suite 150, Woodland Hills, California 91367.

49. Defendants jointly participate in the operation of their pornographic websites. For example, as explained in a 2019 presentation written by Defendants, the Cyprus Companies “oversee[] and manage[] [Defendants’] principal operations including hosting, content, material contracts and arrangements, sales, marketing, billing and collection.” Furthermore, the Cyprus Companies are “the contracting party with all of [Defendants’] customers.”

50. The Cyprus Companies also operate and provide office, legal, moderation, compliance, accounting, and engineering services for the Tube Sites and the Pay Sites. For example, Defendant AYLO Freesites Ltd. operates the Tube Sites and Defendant AYLO Premium Ltd. operates the Pay Sites. Defendant Donormass Ltd. selects and purchases pornographic content for the Tube Sites and the Pay Sites, and it assigns the rights to that content to the appropriate operating entity (*i.e.*, Defendant AYLO Freesites Ltd. or Defendant AYLO Premium Ltd.). And Defendant AYLO Group Holdings Ltd. employs Defendants’ Moderation team, which carries out the moderation practices for all of the Pay Sites and Tube Sites.

51. The Canadian Companies and the U.S. Companies “provide[] day-to-day management services with respect to [Defendants’] operations” and “provide[] the workforce required to carry [out] certain [of Defendants’] functions including[] human resources, information technology, accounting and administration” in return for servicing fees from the Cyprus Companies. For example, Defendant FTSA, LLC facilitates financial transfers between Defendants.

52. The Canadian Companies also provide office, legal, accounting, and engineering services for the Tube Sites and the Pay Sites. For example, besides employing most of Defendants’ executives, Defendant 9219-1568 Quebec Inc. also employs the head of Defendants’ “Trust and

Safety”² team, as well as most of the team itself, which administers one set of policies, practices, and procedures for all Defendants. These policies, practices, and procedures are intended to identify, flag, remove, review, prevent, and report illegal or abusive content, including NCM and CSAM. The Canadian Companies also employ the majority of Defendants’ Compliance team, which services all of the Pay Sites and Tube Sites.

53. Defendant AYLO Global Entertainment Inc. employs Defendants’ Director of Operations for Trust and Safety, as well as their Manager of Operations and Child Safety, who is also a member of the Trust and Safety team. Despite being employed by one of the U.S. Companies, and living in the United States, the Manager of Operations and Child Safety lists the Canadian Companies’ address as her office address.

54. Defendant AYLO Billing Limited handles billing for, and maintains relationships with, European-based acquiring and processing entities in support of the Tube Sites and the Pay Sites.

55. Defendants also regularly commingle funds and transfer funds between themselves. For example, the Cyprus Companies earn advertising and subscription revenues from the Tube Sites and the Pay Sites; they transfer these funds (1) as intercompany royalties, which are then used to pay, among other things, corporate loans and dividends for all Defendants; and (2) to the Canadian and U.S. Companies as management fees, which are then used to pay operating expenses for services for all Defendants.

² This Complaint uses “Trust and Safety”—a term Defendants use to describe departments internal to Defendants’ corporate entities.

Defendants' Distribution of CSAM and NCM

CSAM and NCM on the Tube Sites

56. Defendants endeavor to draw as much web traffic to the Tube Sites as possible each day to maximize advertising revenue. Defendants also earn referral fees when their users sign up for Content Partners' subscription services via links on Defendants' websites. To increase web traffic and attract subscribers, Defendants encourage the creation of as much popular content as possible for distribution through the Tube Sites, with videos and photos featuring teenagers—which may include CSAM and NCM—being one of the most popular categories of content.

57. Since no later than 2012, Defendants' Content Partner team has directed Content Partners, users, and Models via, among other things, quarterly newsletters to contribute such “teen” content, often CSAM and NCM, to the Tube Sites. For example, in 2018, one of Defendants' Content Partner Account Representatives asked a Content Partner to make videos and photos involving “young girl,” “teen,” “young,” “petite,” “schoolgirl,” “punish,” and “teen strip” to draw more views and subscribers. Similarly, Pornhub's Q3 2019 newsletter specifically encouraged Content Partners, users, and Models to make “Tiny Teen” and “Monster Cock Tiny Teen” videos because they were in high demand. Defendants later backtracked on some of these solicitations, (following negative press reports of CSAM) prohibiting “young girl,” “punish,” and “tiny teen” videos because they often included CSAM.

58. Defendants also coordinate with Content Partners to create content for the Tube Sites. Defendants' in-house “script team” regularly writes scripts for Content Partners' videos. Defendants' Content Partner Account Representatives also regularly provide Content Partners with “optimized titles” on a video-by-video basis, as well as the categories, tags, and thumbnails

for each video (as they do with all content) to draw more views and subscribers. Defendants license the resulting content from the Content Partners. The videos and photos are made available on the Tube Sites through Content Partner-specific “channels.”

59. In addition, in March 2020, Defendants identified a number of CSAM and NCM videos on KeezMovies, SpankWire, and ExtremeTube. Defendants owned or licensed all of the content on these websites, meaning they owned or licensed all of this CSAM and NCM content. The videos had titles such as “Brunette Girl was Raped,” “Drunken passed out young niece gets a creampie,” “Amateur teen after party and fun passed out sex realty [sic] submissive,” “Girl getting gangraped,” and “Giving her a mouthful while she’s passed out drunk.” Rather than remove the videos, Defendants merely edited their titles to remove any suggestion that they contained CSAM or NCM. As a result, consumers continued to view and download these videos.

60. As a result, since 2012, Content Partners, users, and Models have uploaded over 4 million “teen” videos to the Tube Sites, of which tens of thousands of these videos were CSAM and/or NCM. Defendants have then offered consumers playlists of these CSAM and/or NCM videos, with titles such as “less than 18,” “the best collection of young boys,” and “under-age.” Defendants have also regularly promoted videos tagged (often by Defendants themselves) with terms indicating CSAM, including “cp” (code for “child pornography”), “no18,” “young,” and “youngster” on the Tube Sites. These videos have typically remained on the Tube Sites for years, where consumers watched and downloaded them millions of times, bringing in tens of millions of dollars in advertising and referral fees for Defendants.

GirlsDoPorn

61. A well-publicized example of Defendants' monetization of NCM involved U.S.-based Content Partner "GirlsDoPorn." Between 2016 and 2019, Defendants licensed that content from GirlsDoPorn for distribution on Pornhub. The content largely consisted of NCM—women agreed to be recorded engaging in sexual activities on the promise that the videos were for private use only. GirlsDoPorn however uploaded these videos to its Pornhub channel, where Defendants optimized their titles, categories, tags, and thumbnails, thereby attracting traffic and subscribers. Defendants earned approximately \$350,000 in referral fees as a result.

62. Between 2016 and 2019, Defendants received over two dozen content removal requests from women featured in GirlsDoPorn videos, with each requesting the content be removed from Defendants' websites because the videos were NCM. While Defendants would typically take down the video specified in each such request, they left up GirlsDoPorn's other videos and channels.

63. It was only in October 2019, after the owners of GirlsDoPorn were criminally indicted for sex trafficking, that Defendants removed the GirlsDoPorn channels from Pornhub. Even then, however, they left up GirlsDoPorn content that had been uploaded to their websites outside of the channels, *i.e.*, by other users who downloaded content from the GirlsDoPorn channels and then re-uploaded it to Defendants' websites under their own usernames. This was over the objection of senior members of Defendants' Compliance team, who argued that all GirlsDoPorn content was harmful to users, lacked documentation, and was illegal. For example, in a January 2020 internal email, after GirlsDoPorn was found liable for distributing NCM, a senior member of Defendants' Compliance team pleaded for the removal of all GirlsDoPorn content from

Defendants' websites, saying that "they are scums," "[t]hey are bad business" and "[v]ery bad for PR." But Defendants disregarded the warning, keeping the GirlsDoPorn content live.

64. As a result, GirlsDoPorn NCM videos were continuously available on the Tube Sites. In fact, as of September 2021, dozens of GirlsDoPorn NCM videos were available on Pornhub, over 70 of which had been on the site since at least 2017.

Content Audits Reveal That Defendants Distributed CSAM and NCM

65. By early 2020, the press was regularly reporting on Defendants' distribution of CSAM and NCM, but Defendants typically ignored the criticisms. For example, in February 2020, the BBC published an article reporting that Pornhub was full of NCM, including videos titled "teen abused while sleeping," "drunk teen abuse sleeping," "extreme teen abuse," and "teen fucked while sleeping." A senior Trust and Safety employee discounted the reporting in an internal email, saying of the videos: "In some such videos the girl wakes up and is clearly enjoying it," while acknowledging others were problematic because "it's not clear if the girl is conscious at all throughout." A senior member of the Tube Sites team declined to remove the videos, explaining in an internal email that, although the videos could be problematic, removing them "hurts us . . . when our competitors allow it."

66. It was only in early 2020, after such reports caused Visa and MasterCard to threaten to terminate their relationships with Defendants and impose massive fines, that Defendants took some modest action. This included auditing the Tube Sites and Pornhub Premium, a Pay Site that contains content from both individuals (specifically solicited by Defendants) and Content Partners, as well as content selected, purchased, and uploaded by Defendants themselves. Unsurprisingly, and as detailed below, these audits turned up tens of thousands of CSAM and

NCM videos and photos—all content that Defendants solicited for upload to the Tube Sites and Pornhub Premium. These videos and photos had been viewed and downloaded millions of times.

Content Partner and Channel Audit

67. In June 2020, MasterCard threatened to fine Defendants \$400,000 for a Content Partner’s channel titled “PunishTeens” because it included “Rape/Brutality.” Defendants’ head of Compliance, who was also effectively the head of Trust and Safety (and, as a senior Trust and Safety employee testified, “the foremost expert in MindGeek on Trust and Safety”), proposed removing the channel because it was NCM. Defendants thereafter removed the channel and all associated videos from Pornhub and Pornhub Premium to avoid the fine; however, Defendants allowed the same content to remain live on their other websites.

68. Defendants’ head of Compliance thereafter ordered an audit of all Content Partners and their channels to identify CSAM and NCM on their channels. The audit identified 35 channels on Pornhub and Pornhub Premium for removal because, according to the audit, their content included “Incest,” “Force,” “Non-consent,” “Violence,” “Spy Cam,” “Revenge Porn,” “Slavery,” and “underage concerns.”

69. For example, the audit identified a channel titled “boys for sale” by Content Partner “CarnalCash” for removal because, according to Defendants’ internal analysis, it featured “Slavery” and raised “underage concerns.” Furthermore, the channel had been advertised on Pornhub since March 2019 as follows: “There’s an underground secret society of men who buy and sell boy slaves on the black market” and “once groomed by the society they are prepared for a life of servicing the men who buy and use and breed their young vi[r]ginal bodies.”

70. The audit also identified for removal a channel titled “Shoplyfter” which advertised itself as containing videos of teens who have been caught shoplifting and store employees “mak[ing] sure these rebellious juveniles never steal again by ANY MEANS NECESSARY.” The channel contained videos with titles such as “Cute Teen Fucks Guard To Avoid Jail.”

71. In addition, the audit flagged for removal channels titled “bathroom creepers,” “boy creeper,” “brutal-x,” “helpless boys,” “helpless teens,” “teen creeper,” “shower spy cameras,” and “shamed sluts” because the channels’ videos included, in Defendants’ own words, “Revenge content,” “Force,” “Violence,” “Hidden Camera,” and “Absence of consent.” The audit also identified channels titled “fragile slave,” “slaves 4 cash,” “young throats,” “brutal invasion,” “defiled 18,” and “HouseofTaboo” as having CSAM and NCM videos and photos, both of which had issues including, in Defendants’ own words, “Non-consent,” “Brutal,” “Force,” “Distress,” “Unconscious,” and “Underage.”

72. As before, Defendants suspended the channels from Pornhub and Pornhub Premium to avoid incurring any fines from credit card companies, but they later restored most of the channels and their content once the threat had passed. As a result, Defendants banned only three Content Partners’ channels for CSAM and two channels for NCM, leaving roughly 30 channels, including “bathroom creepers,” “boy creeper,” “boys for sale,” “brutal-x,” “helpless boys,” “helpless teens,” “teen creeper,” “Shoplyfter,” and “shower spy cameras,” to continue operating and posting content to Pornhub.

73. Defendants maintained these channels over the objection of the head of Compliance, who stated, for example, that all “Shoplyfter” videos were NCM because the women in the videos “appear[] reluctant to do anything. The only possible conclusion a viewer can draw is that she is

being coerced.” He added that Defendants had “cut[] compliance out of this process” and “re-enabl[ed] a channel we agreed should be removed.” And a senior member of the Compliance team echoed this, stating that “the girls never enjoy the sex and only do it to get out of trouble” and the Content Partner should therefore be banned “once and for all.”

74. Similarly, the audit identified a channel titled “NebraskaCoeds,” which contained hundreds of videos that, according to Defendants’ analysis, included “children,” “Intoxication,” “Underage,” “Non-consent,” “Violence,” and “Incest” content. While Defendants removed what they identified as illegal content, they continued publishing content from the Content Partner and distributing it through the channel.

75. During this time, Defendants also did little to review any documentation as to the legality of Content Partners’ content. Professional producers of sexually explicit material are required, pursuant to 18 U.S.C. § 2257, to maintain documentation proving the name and date of birth of each performer in that content. However, in January 2021 Defendants asked their Content Partners to produce this documentation, and over 700 of the Content Partners (out of approximately 3,800 in total) were unable to provide the required documentation for thousands of videos which had been live on the Tube Sites for years, forcing Defendants to take the videos down because they could not verify the name or date of birth of performers in that content.

76. Defendants’ superficial efforts to police CSAM and NCM on their websites are further demonstrated by a March 2021 audit of channel titles. The audit, overseen by Defendants’ Manager of Operations and Child Safety (a senior Trust and Safety employee), identified 37 channels with titles suggesting that they contained CSAM and/or NCM, including “GF Revenge,” “Hardcore Punishments,” “Punished Brats,” and “Bad Teens Punished,” as well as

“Helpless Boys” and “Helpless Teens,” which both had been flagged for removal in the aforementioned 2020 channel audit. While the Manager of Operations and Child Safety testified that “[girlfriend] Revenge” connoted “revenge porn,” that the term “punish” suggested that the channel contained NCM, and that “Helpless Teens” implied that the channel contained CSAM, neither she nor anyone else reviewed or removed the actual videos on the channels. Instead Defendants merely changed the channel titles to make the content appear not to be CSAM or NCM.

General Content Audits

77. In June 2020, Defendants’ head of Compliance ordered an audit of all videos and photos on Pornhub Premium and the Tube Sites.

78. **Pornhub Premium:** Defendants first reviewed a sample of videos on Pornhub Premium and were “confident in the validity of the estimate” that the site contained approximately 2,400 NCM videos and 1,100 CSAM videos.

79. Defendants’ Compliance team subsequently audited all Pornhub Premium content and, as a result, deactivated over 300,000 videos—including videos that Defendants solicited or selected, purchased, and uploaded themselves—for violating Defendants’ terms of service, some of which were CSAM and NCM. These videos had been viewed and downloaded millions of times. A senior member of Defendants’ Compliance team stated in an internal email that “none of it is enough,” “this is just a start,” and “we need to block millions more” because “the site is FULL of non-compliant content.” Another senior employee responded: “it’s over” and “we’re fucked.” The senior Compliance employee added that Pornhub was similarly “full of” non-compliant videos.

80. **Pornhub:** In June 2020, Defendants' Compliance team also initiated an audit of all content on the Tube Sites, first scanning the sites for videos and photos that had previously been "fingerprinted" as CSAM. Upon discovery of CSAM, numerous companies and organizations assign it a "fingerprint," which is an alphanumeric digital identifier unique to the relevant video or image, and lists of those fingerprints are shared among companies and organizations to better identify and prevent the dissemination of CSAM. Defendants' scan found over 1,300 such "fingerprinted" CSAM videos, all of which had been available on Pornhub for over a year (and viewed and downloaded thousands of times), as well as over 4,000 CSAM images. Around the same time, a senior member of Defendants' Compliance team told the head of Compliance in an internal chat that he had "found a goldmine" of "rape content" live on Pornhub.

81. The audit next involved a manual review of every video on the Tube Sites. However, the Tube Sites team generally resisted any efforts by the Compliance or Trust and Safety teams to remove content, even CSAM and NCM, from the Tube Sites. In fact, the Tube Sites team routinely ignored decisions by the head of Compliance with respect to the removal of content from the Tube Sites.

82. With respect to the audit, the Tube Sites team's refusal to remove content resulted in thousands of CSAM and NCM videos remaining live. Indeed, the Tube Sites team refused to remove the same videos from the Tube Sites that the Compliance team had removed from Pornhub Premium as CSAM and NCM. For example, in July 2020, the Compliance team removed a video titled "Helpless Teen Forcefully Fucking Inside Car" from Pornhub Premium as NCM, but the Tube Sites team kept it live on Pornhub.

83. In September 2020, the head of Compliance wrote to the Tube Sites team regarding its refusal to remove CSAM and NCM identified in the audit, stating: “there is content from our review phases that has been confirmed as a violation of compliance rules, but has not been removed.” But the Tube Sites team held strong in its refusals to remove violative content from the Tube Sites. Notably, the Tube Sites were earning over \$300,000 per month on “teen” content.

84. Similarly, in November and December 2020, the Compliance team removed 1,900 videos from the Tube Sites, the majority of which were CSAM and NCM. But, again, the Tube Sites team exercised its authority over the Compliance team and overruled the decision, restoring over half of the videos to the Tube Sites, where at least some of them continue to be available.

85. Despite the continued resistance, the Compliance team’s audit of the Tube Sites led to the removal of over 8,900 CSAM videos between June and December 2020; most of these videos had been available on the websites for years, and consumers had viewed and downloaded them tens or hundreds of thousands of times. Thousands of these videos were titled or tagged with terms suggesting that the videos contained CSAM, including “teen,” “young,” and “petite” videos that Defendants had specifically encouraged the creation of for years. For example, a video titled “High School Latina Teen Flashing Perfect Body on Snapchat” was uploaded in January 2020, and consumers viewed it over 70,000 times before, in August 2020, Defendants took it down as CSAM. Another video, titled “Daughter Blows Step-Dad In Car” was uploaded in September 2017 and tagged “teenager,” “young,” “daughter,” and “dad fucks daughter;” consumers watched the video over 30,000 times before Defendants took it down as CSAM in September 2020.

86. The audit also removed over 347,000 NCM videos from the Tube Sites. Over 40,000 of these videos had been live for at least a year, and consumers viewed and downloaded many of them hundreds of thousands or millions of times. For example, a video titled “school girl abused in bus,” which had been uploaded in July 2017 and tagged “teenager” and “young,” was live until 2020, with consumers watching it over 4 million times. Another video, titled “Young Slut Tricked Into Showing Pussy on Snapchat,” was uploaded in April 2019 and tagged “snapchat,” “young,” and “teen”; consumers viewed it over 600,000 times by the time Defendants removed it as NCM in July 2020.

Pornhub Comes Under Increased Scrutiny

87. In December 2020, The New York Times published an Op-Ed titled “The Children of Pornhub,” which alleged that Pornhub was “infested with rape videos” and “monetize[d] child rapes, revenge pornography, spy cam videos of women showering, racist and misogynist content, and footage of women being asphyxiated in plastic bags.” In an internal email shortly thereafter, Defendants’ Senior Director of Payments, Risk, Fraud & Business Analytics stated that, with respect to illegal content, Pornhub and Pornhub Premium “have always been the problem and we all knew it.”

88. In response, Defendants removed over 10.5 million videos from Pornhub and limited future uploads to Content Partners and individuals who submitted documentation to establish their identities (but not the identity, age, or consent of any individuals in the videos besides the uploader). Defendants also removed the ability for consumers to download most videos.

89. Even after removing so much content, Defendants’ sites continue to contain CSAM and NCM. Over the course of 2021, Defendants identified another 10,000 CSAM and 3,600 NCM

videos on their websites. Thousands of these videos had been available for over a year and included titles like “middle school brow [sic] job,” tagged “blow job” and “middle school”; “Teen doing a handjob after class”; “TEEN JERKS OFF AT SCHOOL (Male) (snapchat . . .),” tagged “school,” “teen,” “risky,” and “sneaky”; and “teen force to get node [sic],” tagged “teenager,” “young,” and “force.”

Defendants’ Actions Caused or Are Likely to Cause Injury to Consumers

90. Defendants’ distribution of CSAM and NCM have caused or are likely to cause consumers substantial injury. First, Defendants’ distribution of CSAM and NCM has caused or is likely to cause substantial injury to the children and non-consenting individuals featured in that content. Indeed, Defendants’ Manager of Operations and Child Safety testified at a 2023 investigational hearing that the distribution of CSAM and NCM “revictimizes” the individuals who were “abused” in the creation of the content.

91. Second, most consumers do not want to view or possess CSAM or NCM. As an initial matter, the viewing or possession of CSAM exposes one to civil and criminal liability in the United States. Thus, Defendants’ exposure of consumers to CSAM and NCM, especially when Defendants misrepresent that such content does not exist on their websites, induces consumers to unknowingly engage in potentially unlawful conduct. And, even beyond the legal liability aspect, Defendants’ own marketing promises consumers that their websites would not carry such content, further establishing this content’s undesirability for the broader market. Exposing consumers to such content is also likely to cause them trauma and emotional distress.

92. These harms were not reasonably avoidable by consumers. With respect to those individuals featured in CSAM and NCM, they could not reasonably avoid the harm because the

content, by its very nature, was made and/or distributed without their consent—these individuals were children, rape victims, spycam victims, or those who did not consent to the content being posted online (*e.g.*, revenge porn). And, as to users of Defendants’ websites, it was not apparent to consumers that they were viewing and/or downloading CSAM or NCM. And, as detailed below, Defendants misrepresent their efforts to keep CSAM and NCM off their websites, giving consumers the false impression that the websites are free from such content.

93. These harms are not outweighed by countervailing benefits to consumers or competition. Defendants’ distribution of CSAM and NCM, and their exposure of consumers to such content, renders no legally cognizable benefits whatsoever to consumers or competition. The creation and distribution of such content is a crime in most jurisdictions, and it is seen as reprehensible by most consumers. Furthermore, the creation of such content regularly victimizes the very individuals featured in it, and its distribution revictimizes such individuals. Therefore, Defendants have no reasonable claim that their actions had any benefit to consumers, let alone that such benefits outweighed the harms inflicted on to the consumers who unwittingly viewed and/or downloaded the content, or those victimized by its creation and distribution.

Defendants’ Deceptive Claims That They Protect Consumers from CSAM and NCM

94. Defendants’ continued monetization of CSAM and NCM has led to repeated public criticism and negative press over the years. To head off the damage this reporting could do to its profits, Defendants have, since 2018, made numerous misrepresentations to burnish their image as good public citizens and to portray their websites hosting only legal pornographic content. In particular, Defendants have falsely promised consumers, both in the press and on their websites, that they will (1) provide the ability to flag violative content for immediate review and removal,

(2) ban users who upload CSAM from their websites, (3) prevent the re-upload of CSAM they have removed from their websites, (4) maintain statutorily required paperwork establishing the age and consent of performers for content on the Pay Sites, (5) review all content to ensure it does not contain CSAM or NCM before it goes live on their websites, and (6) keep CSAM and NCM off their websites. Defendants falsely promise consumers that they engage in these good faith efforts to keep their websites free from such content to distinguish them from other pornography websites, which reportedly also include such content.

95. Defendants' promises give consumers the false impression that their websites are free from CSAM and NCM. Consumers rely on these deceitful statements, leading them to unknowingly view and/or download CSAM and NCM.

Misrepresentations About Reviewing User Flags

96. Since 2018, in response to repeated news reports of CSAM and NCM on their websites, Defendants have told consumers that they can "flag" such content for review and removal. Defendants have repeatedly promised that they will quickly review flagged content, and that they will remove any content found to violate their terms of service, including CSAM and NCM, from their websites.

97. In January 2018, Defendants released a statement to Newsweek UK and GQ magazine stating that "[c]ontent that is flagged on Pornhub that directly violates our Terms of Service [(\"TOS\")] is removed as soon as we are made aware of it; this includes non-consensual content." Similarly, a November 24, 2018, blog post on Pornhub, titled "Answers to Community Questions," stated: "We have a dedicated community that works actively to ensure that content adheres to our TOS and rapidly flags anything questionable for review/removal."

98. In October 2019, in response to reports that NCM videos of women showering were available on Pornhub, Defendants told Jezebel: “Content flagged by our community as inappropriate is promptly reviewed and removed if necessary.” In January 2020, Defendants’ statements, published on BuzzFeed and the Daily Wire, stated that “[c]ontent that is flagged on Pornhub that directly violates our Terms of Service is removed immediately; this includes non-consensual content.” And, around the same time, in response to reports that NCM content featuring U.S. servicemembers through a bathroom peephole had been posted on Pornhub, Defendants told the New York Post: “Here at Pornhub, we immediately remove any content that violates our terms of use as soon as we are made aware of it” and that “users can flag content for review directly on video pages.” Notably, at the same time Defendants were promising consumers the ability to flag CSAM and NCM for quick review and removal, the Tube Sites team was, as detailed above, repeatedly overturning decisions by Defendants’ Compliance team to remove CSAM and NCM from the Tube Sites.

99. Between February and May 2020, Defendants repeatedly told merchant acquirers for Visa and MasterCard that “to combat the proliferation of illegal content, users are encouraged to flag videos deemed inappropriate. These are immediately reviewed by the Pornhub compliance team and removed if they violate the website’s terms of service.” Similarly, in a June 2020 letter to merchant acquirer Merrick Bank, Defendants stated: “Community flagging gives visitors to our websites the ability to flag content that they consider inappropriate. Flagged content is reviewed by a compliance agent and removed from the site if confirmed as a violation.”

100. In September 2020, Defendants deployed an automated response to consumers inquiring about the flagging process, which stated that flagging a video will “initiate the process to have

our team of moderators review the flagged content. . . . Please know that where flagged videos violate our Terms of Service, we will remove them.”

101. The Manager of Operations and Child Safety on Defendants’ Trust and Safety team testified that user flags “play an important role” in detecting and removing CSAM and NCM from Defendants’ websites. She explained that Defendants should review flags “as soon as we can” because “if the content were to be CSAM, NCM, or otherwise violate our terms of service, we would want to remove it.”

102. Nevertheless, from no later than 2015 to May 2020, Defendants’ actual policy was only to review a video once it had received more than 15 separate user flags. Thus, Defendants did not review most flagged content at all, let alone “promptly.” And they did not “immediately” remove content flagged as violative—rather only when it had been flagged more than 15 times would Defendants review the content, and Defendants would only remove the content after that review determined it contained problematic content.

103. As a result, consumers flagged videos as CSAM and NCM over and over again, only for Defendants to ignore those flags for years. Between 2012 and May 2020, Defendants amassed a backlog of over 700,000 active Pornhub videos with up to 15 user flags that had never been reviewed, with many of these flags dating back to 2015. Despite these flags, many of which were for CSAM or NCM, Defendants allowed the videos to remain live on their websites, where consumers continued to view and download them and Defendants continued to earn revenues from them.

104. In June 2020, Defendants finally began reviewing the backlog of flagged videos (though it kept the 700,000 flagged videos live during the review), quickly finding that almost 14,000 of

the videos had been flagged as “underage.” By August 2020, Defendants had reviewed 70,000 of the flagged videos, removing 30% of those videos flagged as “underage” because they were CSAM.

105. At the same time, Defendants were still misrepresenting their review of flags to merchant acquirers to avoid costly fines. For example, in August 2020, Defendants told an acquirer for MasterCard that “all flagged content is reviewed within 24 hours.” This claim omitted the backlog, which, at the time, still amounted to over 600,000 flagged videos (which were still live on Defendants’ websites).

106. Defendants ended up deactivating most of the backlog flagged videos in December 2020 when they took all user-generated content off of their websites. By the time Defendants finally finished reviewing the entire backlog in July 2021, they had identified thousands of CSAM videos and tens of thousands of NCM videos—many of which had been on Pornhub for well over a decade.

Misrepresentations About Banning Uploaders of CSAM

107. Defendants have also falsely promised to ban individuals who upload CSAM to their websites. Specifically, an April 2020 Pornhub blog titled “Answers to Community Questions” stated: “If we ever come across CSAM, the videos are fingerprinted so they cannot be reuploaded, and the user is banned”

108. However, Defendants have repeatedly allowed uploaders of CSAM to continue using, and uploading content to, their websites. For example, in October 2019, a 16-year-old girl repeatedly asked Defendants to ban a Content Partner named “kingdickflash” who had uploaded CSAM of her to Pornhub, stating: “I can prove I am a minor by sending a picture of my state and

school ID. Please get back to me as soon as possible. I'm so scared and nervous. Please I'm begging you. This man is preying on young girls. I did not give consent to him. Nor did I know he was recording. The other videos on his page are most likely girls my age or younger." While Defendants took down the video in question as CSAM, as well as several of the Content Partner's other videos, the Tube Sites team directed the Compliance team not to ban the Content Partner or channel, allowing it to continue posting videos until January 2021.

109. Similarly, and as noted above, Defendants did not ban a Content Partner with a channel titled "NebraskaCoeds" despite the channel having hundreds of videos which, by Defendants' own 2020 description, included "children" and "underage."

110. As another example, although a Content Partner with the username "exploitedteenasian" had, according to Defendants' Compliance manager, a "past history of uploading underage content," Defendants allowed it to continue acting as a Content Partner and upload content to Defendants' sites until at least December 7, 2020.

111. Separately, Defendants did not cross-ban CSAM uploaders across their websites until June 2021, meaning that when a user was banned from one of Defendants' websites for uploading CSAM, Defendants did not ban the user from any of their other websites even when they used the same email address and username on Defendants' other websites. When Defendants did finally begin cross-banning CSAM uploaders across their websites, they found at least 20 active Pornhub users who had previously been banned from RedTube or YouPorn for uploading CSAM.

112. Moreover, until October 2022, even when Defendants did ban a CSAM uploader, Defendants merely prohibited the user from making a new account under the same username or

email address. However, individuals regularly circumvented such “bans” by using an alternate email address and username; and Defendants knew that individuals routinely evaded their “bans” through this practice. As a result, numerous “banned” users created new accounts and continued to upload CSAM to Defendants’ websites, where unsuspecting consumers continued to view and download the content.

Misrepresentations About Preventing the Re-Upload of CSAM

113. Defendants have also falsely promised that they prevent CSAM from ever being re-uploaded to their websites. Indeed, an April 2020 Pornhub blog titled “Answers to Community Questions” stated: “If we ever come across CSAM, the videos are fingerprinted so they cannot be reuploaded”

114. However, between at least 2017 and August 2021, Defendants’ technology for fingerprinting and preventing the re-upload of CSAM did not work effectively. As a result, hundreds of videos that had previously been identified as CSAM were re-uploaded to Defendants’ websites, where they remained live for months before Defendants took them down again.

115. Defendants knew of the problem as far back as November 2020, when one of Defendants’ employees told the vendor for the fingerprinting technology that Defendants were encountering “a large number of videos falsely labeled as non matches on Pornhub.”

Misrepresentations About Documentation of Age and Identity

116. Defendants have, since at least 2012, also falsely promised users of each of their Pay Sites (including Pornhub Premium) that, for all content on that site, Defendants “obtain[], review[], verif[y], and maintain[] a copy of the 2257 documentation providing that performers

are of legal age” and such documentation is “physically kept at one of MindGeek’s office locations.” “2257” refers to 18 U.S.C. § 2257, which requires documentation (typically, government-issued identification) proving the name and date of birth of each performer in that content.

117. And in February and May 2020 letters to merchant acquirers representing Visa and MasterCard, Defendants stated that, for the Pay Sites, they “maintain[] thorough 2257 records for all content made available to subscribers.”

118. In truth, until December 2020, Defendants did not require any documentation for any of the user-generated content on Pornhub Premium.

119. And, until January 2021, Defendants failed to maintain identity and age documentation for thousands of their videos on the other Pay Sites. In fact, in January 2021, Defendants audited their identity and age documentation for each of the Pay Sites, finding that they were missing documentation for over 8,000 videos across Pay Sites Mofosex.com, Digitalplayground.com, Realitykings.com, Brazzers.com, Brazzersplus.com, and Seancody.com. Thousands of these videos had been available on the Pay Sites since 2015, and they had been viewed and downloaded thousands of times.

Misrepresentations About Reviewing Content to Prevent CSAM or NCM from Going Live on Defendants’ Websites

120. Since no later than October 2019, Defendants have made repeated false promises, both in statements to the press and on their websites, that their Moderation team reviews all content prior to it going live to ensure that CSAM and NCM do not go live on Defendants’ websites.

Defendants make these claims to dupe consumers into believing that their websites are free from CSAM and NCM.

121. In October 2019, in response to public reporting that NCM spycam videos of women showering were available on Pornhub, Defendants told Jezebel that they employed “a dedicated team of human reviewers to review content uploaded” to their websites.

122. In February 2020, in response to a statement by United States Senator Ben Sasse that Pornhub makes “content available worldwide showing women and girls that were victims of trafficking being raped and exploited,” Defendants stated publicly that they “employ[ed] an extensive team of human moderators dedicated to manually reviewing every single upload.” Defendants’ Chief Legal Officer similarly told United States Senator Maggie Hassan, in a publicly released letter, that Defendants have “an extensive team of human moderators who manually review all uploads to the site.” Around the same time, in response to an online petition to shut down Pornhub, Defendants released a statement that was published by Fox News and the Guardian, stating that Defendants employed “an extensive team of human moderators dedicated to manually reviewing all uploads to the site.”

123. Beginning in April 2020, Defendants published multiple policy documents, statements, and blog posts, making similar false claims that they review all content uploaded to its websites:

- a. An April 2020 Pornhub blog post, titled “Answers to Community Questions,” stated:
“First and foremost, illegal content is strictly prohibited on Pornhub. This has always been the case and will always be the case, and the safety of our users and models is our number one priority. Upon upload, every video and photo uploaded to Pornhub is

reviewed manually by a large and extensive team of moderators looking for illegal content.”

b. Pornhub’s Child Sexual Abuse Material Policy, first published in May 2020, states:

“Pornhub has an extensive team of human moderators who actively work around the clock to review all content uploaded to our platform in order [to] prevent any illegal content from being featured on our platform, [and] remove any content that may violate our terms of service”

c. Pornhub’s Non-Consensual Content Policy, first published in May 2020, states: “We employ an extensive team of moderators and support staff who work 24 hours a day, 7 days a week in order to review all uploaded content for violations, and address users concerns, and remove all non-consensual content that we identify or of which we are made aware.”

d. A December 2020 press release by Defendants stated that “Pornhub’s current moderation includes an extensive team of human moderators dedicated to manually reviewing every single upload.”

124. In truth, at the time Defendants made each of these statements, there were hundreds of thousands of videos on Pornhub that had never been reviewed by the Moderation team. And, until April 2020, Defendants did not review the 5 million videos on Spankwire, MofoSex, ExtremeTube, or KeezMovies at all, even though these sites were all linked to by Pornhub and described as being “in the Pornhub network.” Similarly, Defendants’ Moderation team never reviewed older free videos that had been uploaded to XTube; upon realizing this in December 2020, Defendants deleted the videos rather than reviewing them.

125. Even as to those videos that were reviewed by Defendants' Moderation team, Defendants' policies, practices, and procedures kept their moderators from meaningfully examining the videos and in fact mandated approval of most videos, regardless of the content.

126. Specifically, Defendants limited the number of videos that moderators could remove from Defendants' websites, regardless of the illegality of the content. For example, as of November 2019, Defendants told moderators not to remove more than 0.6% of content uploaded to YouPorn and no more than 0.4% of content uploaded to RedTube.

127. As to the substantive review of videos, a senior Trust and Safety employee who routinely audits decisions by the Moderation team testified that it is "important to view the whole video" and to "listen to it, too" because a moderator could otherwise miss indicators that content is CSAM or NCM, such as an individual stating their age or stating that they are "not consenting to the sexual act." She added that, "[i]deally, a moderator would be able to watch and listen to the entirety of the video." The employee further explained that, in the context of reviewing for CSAM and NCM, "accuracy is more important" than speed because "we would want to ensure fewer mistakes, [and] that content that is NCM or C[SA]M . . . is removed as early as possible." And she acknowledged that, with respect to CSAM and NCM, each "mistake is . . . revictimizing the person who's the subject of the video."

128. For years, however, Defendants have mandated, and continue to mandate, speed over a meaningful and accurate review of content, forcing moderators to review as much content as fast as possible. Specifically, Defendants' policies typically limit the review of each video to one moderator, who can review only a small portion of each video before it goes live. Moreover,

moderators routinely do not listen to the entirety of the video. And, in some instances, moderators do not understand the language spoken in the videos.

129. As a result of Defendants' policies, in 2019, each moderator reviewed, on average, 750 videos and 1,400 photo albums in an eight-hour shift. Setting aside the photos, this amounted to a moderator watching on average, only 39 seconds of each video that they reviewed. At the same time, of the nearly 6 million videos uploaded to Pornhub in 2019, approximately 10% (635,394) were over 30 minutes in length, almost 20% (1,147,672) were between 10 and 30 minutes in length, and another approximately 16% (936,524) were between 5 and 10 minutes in length.

130. Tellingly, Defendants' head of Moderation bragged, in a January 2019 employee evaluation report, that he typically reviewed approximately 1,200 videos each eight-hour shift, meaning he watched, on average, only 24 seconds of each video. He also applauded two other moderators for reviewing 850 and 1,290 videos per eight-hour shift.

131. At the same time that Defendants limited the amount of time a moderator could spend reviewing a video, Defendants specifically encouraged Content Partners, Models, and users, through a publication called "The Pornhub Playbook: How to make money with Pornhub," to make longer videos, stating that "users are far more likely to click longer videos," and "videos of 10 minutes or longer will achieve optimal viewing results."

132. In 2020, Defendants further restricted moderators' ability to review content, with each moderator reviewing, on average, 880 videos and 1,800 photo albums per eight-hour shift. This amounted to each moderator spending, on average, only about 34 seconds on each video. And, of the over 10 million videos uploaded to Pornhub in 2020, about 13% (1,347,255) were over 30

minutes in length, approximately 21% (2,162,445) were 10 to 30 minutes long, and about 18% (1,863,696) were 5 to 10 minutes in length.

133. By April 2020, Defendants' head of Moderation was raising the alarm that the Moderation team was in "panic mode" because it was severely understaffed and, as a result, moderators were making mistakes due to the high volume of videos they were required to review. At the same time, Defendants' head of Compliance recognized, in an internal email, the importance of reviewing the entirety of each video because videos "can be non-compliant based on small segments." He separately stated that the rate of moderation "is super high – obviously it's great to get through the content as fast as possible but we need to be sure enough time is being allocated to each video so nothing is missed."

134. Defendants' policies, practices, and procedures continue to emphasize speed for moderators. As a result, moderators continue to review 300–400 videos per eight-hour shift, meaning they are only capable of reviewing a fraction of each video.

Misrepresentations About the Presence of CSAM and NCM

135. Defendants have repeatedly promised consumers that their aforementioned policies, practices, and procedures work together to ensure there is no CSAM or NCM on their websites. But, as detailed above, Defendants' sites have contained, and continue to contain, such content.

136. Pornhub Premium has always had a notice that states:

All models, actors, actresses and other persons that appear in any visual depiction of actual sexually explicit conduct appearing or otherwise contained in this Website were over the age of eighteen years at the time of the creation of such depictions. With respect to all visual depictions displayed on this website, whether of actual sexually explicit conduct, simulated sexual content or otherwise, all persons in said visual depictions were at least 18 years of age when said visual depictions were created.

137. In February 2020, in response to an inquiry from United States Senator Maggie Hassan, Defendants' Chief Legal Officer stated (in a letter made publicly available): "MindGeek has put in place state-of-the-art, comprehensive safeguards on its platform to combat this material, including a robust system for flagging, reviewing and removing all illegal material."

138. In an April 2020 Pornhub blog titled "Answers to Community Questions," Defendants stated:

First and foremost, illegal content is strictly prohibited on Pornhub. This has always been the case and will always be the case, and the safety of our users and models is our number one priority. Upon upload, every video and photo uploaded to Pornhub is reviewed manually by a large and extensive team of moderators looking for illegal content. In addition, we use automated detection technologies . . . as added layers of protection to keep unauthorized content off the site. Finally, we also review any flags or content removal reports for illegal content. We have a dedicated community that works actively to ensure that content adheres to our TOS and rapidly flags anything questionable for review/removal If we ever come across CSAM, the videos are fingerprinted so they cannot be reuploaded, and the user is banned All illegal content, in addition to content that breaches our Terms of Use, is immediately removed as soon as it is detected.

139. Similarly, Pornhub's Child Sexual Abuse Material Policy, first posted in May 2020, states:

We have a zero-tolerance policy toward child sexual abuse material on our platform, as well as toward those who produce, disseminate, as well as seek out and consume CSAM. Any content featuring or depicting a child is strictly forbidden on our platform and is deemed to constitute a grave violation of our terms of service.

140. In its 2020 Transparency Report, published in April 2021, Defendants stated that they had "a firm zero tolerance policy against underage content." It further stated: "In an on-going effort to ensure that our platform remains free of illegal content, . . . Pornhub moderates user-uploaded content before it is accessible to the public and we continue to monitor content after it

is accessible to the public,” adding: “Our team works around the clock in an effort to prevent unacceptable content from being made available to the public for viewing.” And the report emphasized that illegal content does not make it onto Defendants’ sites, stating: “When a user’s content or platform activity violates our Terms of Service and Related Guidelines, we will not publish the content.”

141. However, as described above in Paragraphs 56–89, Defendants’ websites have contained thousands of CSAM and NCM videos and photos, and consumers have both knowingly and unknowingly viewed and downloaded this content millions of times. Thus, Defendants’ claims that their policies, practices, and procedures ensure that their websites are free from CSAM and NCM are false.

Defendants’ Deceptive Privacy and Security Practices

Defendants’ Deceptive Privacy Omissions

142. Since December 2020, Defendants have repeatedly failed to disclose material information about their collection and retention practices with respect to the personal information of consumers who enroll in Defendants’ Model Program, including their dates of birth, Social Security numbers, and government-issued identification documents.

143. In December 2020, Defendants issued a press release announcing that, going forward, they would use a vendor to verify the identities of individuals seeking to participate in the Model Program (the “Vendor”). This included that the Vendor would collect, review, and secure consumers’ identification documentation and the personal information contained therein.

Defendants issued a press release stating:

Going forward, anyone seeking verification within the Model Program must confirm their identity with a current photo and government-approved

ID document first. [The Vendor] will check the ID document validity and then match the user's ID document to their photo using secure biometric technology. This added layer of protection will make the MindGeek verification system modern, robust and secure.

144. In February 2021, Defendants similarly claimed on their websites that the Vendor would be responsible for collecting and reviewing consumers' identification documents: "In order to be eligible to upload content and receive earnings in the Model Program, you need to verify your identity. To complete your identity verification, please follow the steps below from [the Vendor]."

145. Pornhub's 2020 and 2021 Transparency Reports, published in 2021 and 2022 respectively, also stated that Pornhub used the Vendor to collect, verify, and secure consumers' identification documentation: "Users who verify their age with [the Vendor] can trust that their personal data remains secure. [The Vendor] is certified to meet the requirements of ISO/IEC 27001, which is the global gold standard for information security management. This means that [the Vendor's] security aligns with Pornhub's commitment to protecting our users' privacy as well."

146. Consumers have stated to Defendants that they do not trust Defendants with their personal information, so promises that the Vendor will handle and secure their identification documentation are material to them. Indeed, consumers have routinely stated concerns such as "this is private and personal information that I don't feel comfortable uploading to a site like [Pornhub]."

147. What Defendants fail to tell consumers, however, is that when consumers enrolling in the Model Program submit their verification documentation—which routinely includes their driver's

licenses and passports—to the Vendor, the documentation is then passed to Defendants, and they hold it in an internal database without the consumers’ knowledge or consent.

148. In addition, Defendants hold this information in perpetuity, with no internal policy or procedure governing when, if ever, the information should be deleted. Defendants even falsely promise to delete the accounts of Models upon request. In reality, a senior employee in Defendants’ Model Program explained in an internal email: “[W]e don’t truly delete any accounts Models however believe it’s deleted since all their info and content is removed from the front end.” Indeed, Defendants even tell Models that they will delete their identification documentation upon request, only to merely archive the documents for later possible retrieval.

Defendants’ Deceptive Information Security Practices

149. Defendants’ statements as to the security employed to protect consumers’ personal information are also false.

150. Between January 2018 and December 2020, Defendants required prospective members of their Model Program to submit “verification images” showing most of their faces, meaning no masks or sunglasses. Defendants also required that the verification images include the prospective Model “holding up a sign with your username and pornhub.com written on it (or write it on your body).” During this time period, Defendants told prospective Models that “[a]ll verification images are totally private, only seen by Pornhub staff and stored securely.”

151. In connection with their use of the Vendor for identity verification (beginning in 2021), Defendants tell prospective Models that they “can trust that their personal data remains secure” and “[the Vendor] is certified to meet the requirements of ISO/IEC 27001, which is the global gold standard for information security management.” And Defendants’ customer service

representatives inform Models that their identification documentation are “completely confidential and secure.”

152. And in recognition of the sensitivity of the documentation it is receiving, Defendants’ own policies require that the documents be stored in a secure database protected by a firewall, with access limited to a few employees whose access is logged.

153. However, since at least 2018, Defendants have engaged in several unreasonable data security practices. Among other things, Defendants regularly disregard their protocols by failing to secure the database storing the identification documents by firewall or similar protection. Defendants’ employees also fail to keep the information secure, instead emailing unencrypted copies of consumers’ verification images, identification documents, passports, driver’s licenses, Social Security numbers, and birth certificates to numerous other employees who are not supposed to have access to the documents. These employees have kept, and continue to keep, the documents in their email accounts, unsecured and in plain text, for years.

154. These practices violate Defendants’ own “Encryption Policy” and “Data Privacy Compliance Statement,” both of which have been in effect since at least June 2019 and which require encryption of this sensitive personal information in transit and at rest. Even the database designated for identification documents is not secured; Defendants do not encrypt consumers’ identification documents, or the personal information contained therein, instead storing them in plain text. Moreover, Defendants do not limit how long they will retain consumers’ personal information, holding it in plain text in the database and in employees’ email accounts in perpetuity.

DEFENDANTS' CONTACTS WITH THE STATE OF UTAH

155. Defendants have significant contact with the state of Utah, which include the following.

156. First, Defendants' websites have been visited by many users located in Utah. This access is not free: Defendants charge Utah consumers either with payment for subscriptions, or by taking their time and information, which it then converts into advertising revenues.

- a. Pornhub's "2017 Year in Review" reported that on average, visitors from Utah are on the site for 10 minutes and 1 second.
- b. Utah consumers have reported CSAM on RedTube and Pornhub to the National Center for Missing & Exploited Children's CyberTipline ("CyberTipline"), demonstrating that Utahns have accessed and viewed content on Defendants' websites.
- c. In 2023, Defendants blocked Utahns from accessing Pornhub and its related sites. The next day, Utah had the most VPN-related searches in the United States as Utahns tried to get around the block.

157. Second, Defendants' websites contain videos that were made in Utah.

- a. Content removed in 2019 from Defendants' Pornhub website as suspected CSAM and/or NCM include the following video titles:
 - i. "Ex Girlfriend [redacted full name] Sucking Cock," tagged as "Utah" and "salt lake city."
 - ii. "Slut [redacted full name] from Utah."
 - iii. "Meth trash slut from Utah ([redacted full name])." Tags included "teen."
 - iv. "Am [redacted full name] live in [redacted full Utah physical address]."

- v. “Utah college boy shoots in the sink.”
- vi. “ - - The Infamous Mormon Girl.” Tags included “Utah” and “amateur.”
- b. Content removed in 2020 from Defendants’ Pornhub website as suspected CSAM and/or NCM included the following video titles:
 - i. “Utah provo video [redacted full name]! Video borrado.” Tags included “Utah.”
 - ii. “[Redacted full name] giving roadhead.” Tags included “amateur,” “Utah,” “amateur Utah,” “Utah slut,” and “Utah milf.”
 - iii. “Georgia man fails at fucking Utah teen on the floor.”
- c. A video with suspected CSAM and/or NCM titled “SF Straight Guys Boston & Utah Get Blowjobs On Cam For Straight Fraternity Fan Viewers” was reuploaded to Defendants’ websites after being taken down.
- d. Defendants are aware of users in Utah uploading images and videos containing CSAM to its sites. For example, in 2021, apparent CSAM was uploaded to Defendants’ sites from users located in various Utah cities, such as Salt Lake City, Clinton, St. George, and Woods Cross.
- e. Detectives, investigators, and police departments in Utah—including from West Valley City, Provo, Sandy, and North Salt Lake City—have contacted Defendants on behalf of Utah victims about revenge pornography and other sex offenses posted to their websites. In one case, the ex-boyfriend of a Utah resident posted several sex videos of her to Pornhub without her consent as part of an ongoing campaign of harassment and intimidation. One video, posted in 2020, had 1,704

views. The ex-boyfriend messaged the Utah resident: “I’m done, No more threats, prove I threatened you, Prove I leaked those images, Oops.” [Utah resident name redacted] reported the incident to North Salt Lake Police Department.

158. Third, content created in Utah has generated revenue for Defendants. For example, in 2020, Defendants profited from content with the following tags: “Utah,” “Utah slut,” “Utah escort,” “Salt Lake City,” “Utah whore,” “Mormon,” and “Mormon boys.”

159. Fourth, Defendants sold advertising space to marketers in Utah.

a. A resident of Salt Lake County, Utah, advertises his services on Pornhub. He also teaches others how to do the same; one of his instructional videos posted online is titled: “400k in 1 month: How to Make Money Online with PornHub.”

b. A resident of Pleasant Grove, Utah, writes gay erotica sold as audiobooks online, and he directs prospective consumers to his products by advertising on Pornhub.

160. Finally, Utahns have enrolled in Defendants’ Model Program and have been featured in pornographic images and videos posted to their websites.

a. Models on Pornhub have usernames suggesting that they live in Utah, for example using the word “utah” in their usernames.

b. Some models list their cities of residence on their public profiles, and several have listed cities of residence in Utah, including Price, Utah and Salt Lake City, Utah.

161. Based on the facts and violations of law alleged in this Complaint, the FTC and the Division have reason to believe that Defendants are violating or about to violate the laws enforced by the FTC and the Division because, among other things, Defendants earned significant revenues from participating in these unlawful acts and practices, Defendants

continued their unlawful acts or practices despite knowledge of numerous complaints, and Defendants remain in the pornographic content business and maintain the means, ability, and incentive to resume their unlawful conduct.

VIOLATIONS OF THE FTC ACT

162. Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), prohibits “unfair or deceptive acts or practices in or affecting commerce.”

163. Misrepresentations or deceptive omissions of material fact constitute deceptive acts or practices prohibited by Section 5(a) of the FTC Act.

164. Acts or practices are unfair under Section 5 of the FTC Act if they cause or are likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition. 15 U.S.C. § 45(n).

COUNT I

Unfairness –Distribution of CSAM and NCM to Consumers

(By Plaintiff Federal Trade Commission)

165. In numerous instances, Defendants have distributed CSAM and NCM on their websites.

166. Defendants’ acts or practices cause or are likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition.

167. Therefore, Defendants’ acts or practices as described in Paragraph 165 constitute unfair acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. § 45(a), (n).

COUNT II

Deception – Flagging of Content

(By Plaintiff Federal Trade Commission)

168. In numerous instances in connection with the advertising, marketing, distribution, or offering for sale of pornographic content, Defendants represented, directly or indirectly, expressly or by implication, that they review and remove content on Defendants' websites that had been flagged by consumers as illegal or otherwise violating Defendants' terms of service, including CSAM and NCM.

169. In fact, in numerous instances in which Defendants have made the representation described in Paragraph 168, Defendants did not review or remove content on Defendants' websites that had been flagged by consumers as illegal or otherwise violating Defendants' terms of service, including CSAM and NCM.

170. Therefore, Defendants' representation as described in Paragraph 168 is false or misleading and constitutes a deceptive act or practice in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

COUNT III

Deception – Banning

(By Plaintiff Federal Trade Commission)

171. In numerous instances in connection with the advertising, marketing, distribution, or offering for sale of pornographic content, Defendants represented, directly or indirectly, expressly or by implication, that they would ban individuals who had uploaded CSAM to any of Defendants' websites from further use of any of Defendants' websites.

172. In fact, in numerous instances in which Defendants have made the representation described in Paragraph 171, Defendants did not ban individuals who had uploaded CSAM to any of their websites from further use of any of Defendants' websites.

173. Therefore, Defendants' representation as described in Paragraph 171 is false or misleading and constitutes a deceptive act or practice in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

COUNT IV

Deception – Re-Upload of CSAM

(By Plaintiff Federal Trade Commission)

174. In numerous instances in connection with the advertising, marketing, distribution, or offering for sale of pornographic content, Defendants represented, directly or indirectly, expressly or by implication, that they would prevent CSAM that they had identified and removed from Defendants' websites from being re-uploaded to any of Defendants' websites.

175. In fact, in numerous instances in which Defendants have made the representation described in Paragraph 174, Defendants did not prevent CSAM that they had identified and removed from Defendants' websites from being re-uploaded to any of Defendants' websites.

176. Therefore, Defendants' representation as described in Paragraph 174 is false or misleading and constitutes a deceptive act or practice in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

COUNT V

Deception – Verification Paperwork

(By Plaintiff Federal Trade Commission)

177. In numerous instances in connection with the advertising, marketing, distribution, or offering for sale of pornographic content, Defendants represented, directly or indirectly, expressly or by implication, that they maintained paperwork required by 18 U.S.C. § 2257 for all videos on the Pay Sites.

178. In fact, in numerous instances in which Defendants have made the representation described in Paragraph 177, Defendants did not maintain paperwork required by 18 U.S.C. § 2257 for all videos on the Pay Sites.

179. Therefore, Defendants' representation as described in Paragraph 177 is false or misleading and constitutes a deceptive act or practice in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

COUNT VI

Deception –Review of Content, Including for CSAM and NCM

(By Plaintiff Federal Trade Commission)

180. In numerous instances in connection with the advertising, marketing, distribution, or offering for sale of pornographic content, Defendants represent, directly or indirectly, expressly or by implication, that they review all videos before the videos go live on any of Defendants' websites and that such review is effective at identifying CSAM and NCM.

181. In fact, in numerous instances in which Defendants have made the representation described in Paragraph 180, Defendants do not review all videos before the videos go live on any

of Defendants' websites and Defendants' review, to the extent it is undertaken, is not effective at identifying CSAM and NCM.

182. Therefore, Defendants' representation as described in Paragraph 180 is false or misleading and constitutes a deceptive act or practice in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

COUNT VII

Deception – CSAM and NCM

(By Plaintiff Federal Trade Commission)

183. In numerous instances in connection with the advertising, marketing, distribution, or offering for sale of pornographic content, Defendants represent, directly or indirectly, expressly or by implication, that Defendants' websites do not contain CSAM or NCM.

184. In fact, in numerous instances in which Defendants have made the representation described in Paragraph 183, Defendants' websites contain CSAM and NCM.

185. Therefore, Defendants' representation as described in Paragraph 183 is false or misleading and constitutes a deceptive act or practice in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

COUNT VIII

Failure to Disclose – Collection of Personal Information

(By Plaintiff Federal Trade Commission)

186. In numerous instances in connection with the advertising, marketing, distribution, or offering for sale of pornographic content, Defendants represent, directly or indirectly, expressly

or by implication, that consumers' sensitive personal information will be collected and maintained by the Vendor and not held by Defendants.

187. In numerous instances when Defendants make the representation described in Paragraph 186, Defendants fail to disclose, or fail to disclose adequately to consumers that Defendants collect and retain consumers' sensitive personal information from the Vendor. This fact would be material to consumers in their conduct regarding the pornographic content.

188. In light of the representation set forth in Paragraph 186, Defendants' failure to disclose or disclose adequately the material information as described in Paragraph 187 constitutes a deceptive act or practice in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

COUNT IX

Security Misrepresentation – Data Security

(By Plaintiff Federal Trade Commission)

189. In numerous instances in connection with the advertising, marketing, distribution, or offering for sale of pornographic content, Defendants represent, directly or indirectly, expressly or by implication, that Defendants take reasonable precautions to protect the personal information Defendants collect from consumers or via the Vendor.

190. In fact, in numerous instances in which Defendants have made the representation described in Paragraph 189, Defendants fail to take reasonable precautions to protect the personal information Defendants collect from consumers or via the Vendor.

191. Therefore, Defendants' representation as described in Paragraph 189 is false or misleading and constitutes a deceptive act or practice in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

VIOLATIONS OF THE UCSPA

192. The UCSPA prohibits suppliers from committing deceptive and unconscionable acts or practices in connection with a consumer transaction, whether the act occurs before, during, or after the transaction. Utah Code §§ 13-11-4(1); 13-11-5(1).

193. The services Defendants provide are disposed to users for personal purposes and are therefore consumer transactions. Utah Code §§ 13-11-3(2), (5).

194. Defendants regularly and in the ordinary course of business provide these services for consumers and are therefore suppliers under the UCSPA. Utah Code § 13-11-3(6).

COUNT X

Unconscionable Acts and Practices

(By Plaintiff Utah Division of Consumer Protection)

195. By engaging in the acts and practices alleged in this Complaint, Defendants engaged in unconscionable acts and practices that affected Utah consumers in violation of the UCSPA, Utah Code § 13-11-5.

196. Defendants have distributed CSAM and NCM on their websites, perpetuating the sexual abuse of children and adults.

197. Defendants knew or had reason to know those actions substantially contributed to or caused injuries to their consumers as well as the children and adults featured in CSAM and/or NCM. Defendants' actions served to maximize their financial gain at the expense of the consumers and other victims.

198. Defendants knew or had reason to know that they exposed consumers to content containing CSAM and/or NCM despite the fact that most consumers do not want to view such

content or be complicit in the practices that create such content. Viewing CSAM or NCM is likely to cause trauma, emotional distress, stigma, and/or embarrassment.

199. Defendants knew or had reason to know that they exposed consumers to content containing CSAM, even though viewing and possessing CSAM exposes consumers to civil and criminal liability.

200. The above acts and practices are unconscionable in violation of the UCSPA.

201. Defendants' unlawful and unconscionable acts targeted and affected Utah residents.

COUNT XI

Deceptive Acts and Practices

(By Plaintiff Utah Division of Consumer Protection)

202. By engaging in the acts and practices alleged in this Complaint, Defendants engaged in deceptive acts or practices affecting Utah consumers, including by making or causing to be made to Utah consumers, directly or indirectly, explicitly or by implication, misrepresentations of material facts in violation of the UCSPA, Utah Code § 13-11-4.

203. Defendants made or caused to be made to Utah consumers, directly or indirectly, explicitly or by implication, misrepresentations that violate the UCSPA under at least, Utah Code § 13-11-4(1), (2)(a–b, e); by:

- a. Misrepresenting that they reviewed and removed content on Defendants' websites that had been flagged by consumers as illegal or otherwise violating Defendants' terms of service;
- b. Misrepresenting that they banned individuals who had uploaded CSAM to any of Defendants' websites from further use of any of Defendants' websites;

- c. Misrepresenting that they would prevent CSAM that Defendants had identified and removed from Defendants' websites from being re-uploaded to any of Defendants' websites;
- d. Misrepresenting that they maintained documentation required by 18 U.S.C. § 2257 for all videos on the Pay Sites;
- e. Misrepresenting that they review all videos before the videos go live on any of Defendants' websites and that such review is effective at identifying CSAM and NCM;
- f. Misrepresenting that their websites do not contain CSAM or NCM;
- g. Misrepresenting that consumers' sensitive personal information will be collected and maintained by the Vendor and not held by Defendants; and
- h. Misrepresenting that Defendants take reasonable precautions to protect the personal information Defendants collect from consumers or via the Vendor.

204. Defendants knowingly made the above misrepresentations and engaged in deceptive practices in violation of the UCSPA.

205. Defendants' acts and practices were deceptive and violate the UCSPA. These deceptive and unlawful acts targeted and affected Utah residents.

CONSUMER INJURY

206. Consumers are suffering, have suffered, and will continue to suffer substantial injury as a result of Defendants' violations of the FTC Act and the UCSPA. In addition, Defendants have been unjustly enriched as a result of their unlawful acts or practices. Absent injunctive relief by this Court, Defendants are likely to continue to injure consumers and harm the public interest.

PRAYER FOR RELIEF

Wherefore, the FTC and the Division request that the Court:

- A. Enter a permanent injunction to prevent future violations of the FTC Act and the UCSPA;
- B. Order Defendants to pay civil penalties and fines to the Utah Division of Consumer Protection for their violations of the UCSPA; and
- C. Award any additional relief as the court determines to be just and proper.

Respectfully submitted,

Dated: 09/03/2025

/s/ Jacqueline Ford
Jacqueline Ford
Manmeet Dhindsa
Alejandro Rosenberg
(Each appearing pursuant to DUCivR 83-1.1(b)(1))
Federal Trade Commission
600 Pennsylvania Ave., N.W., CC-6316
Washington, D.C. 20580
Telephone: (202) 326-2844
jford1@ftc.gov
mdhindsa@ftc.gov
arosenberg@ftc.gov

Attorneys for Plaintiff
FEDERAL TRADE COMMISSION

/s/ Douglas Crapo
Douglas Crapo (14620)
Stevenson Smith (18546)
Carina Wells (19112)
Utah Attorney General's Office
160 East 300 South, Fifth Floor
Salt Lake City, UT 84114
Telephone: (801) 366-0310
crapo@agutah.gov
scsmith@agutah.gov
cwells@agutah.gov

Attorneys for Plaintiff
UTAH DIVISION OF CONSUMER
PROTECTION