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,

STIPULATED ORDER FOR PERMANENT INJUNCTION, MONETARY JUDGMENT, AND OTHER RELIEF[1]

Case No. 2:25-cv-00752

Judge Ted Stewart

[1] CONTENT WARNING: This Order contains references to, and descriptions of, various sensitive content, including pornographic content, sexually explicit content involving minors, 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 ("Commission" or "FTC") and the Utah Division of Consumer Protection ("Division"), jointly filed their Complaint for Permanent Injunction, Monetary Judgment, and Other Relief ("Complaint") for a permanent injunction, monetary relief, and other relief in this matter pursuant to Section 13(b) of the FTC Act, 15 U.S.C. § 53(b), and the Utah Consumer Sales Practices Act ("UCSPA"), Utah Code § 13-11-1 *et seq*. The Commission, the Division, and Defendants AYLO Group Ltd.; Donormass Limited; AYLO Freesites Ltd.; AYLO Premium Ltd.; AYLO Technologies Ltd.; 9279-2738 Quebec Inc.; 9219-1568 Quebec Inc.; AYLO Holdings USA Corp.; AYLO Billing US Corp.; Toqon, LLC; AYLO Global Entertainment Inc.; AYLO USA Incorporated; FTSA, LLC; and AYLO Billing Limited (collectively "Defendants") stipulate to the entry of this Order for Permanent Injunction, Monetary Judgment, and Other Relief ("Order") to resolve all matters in dispute in this action between them.

THEREFORE, IT IS ORDERED as follows:

FINDINGS

1. This Court has jurisdiction over this matter.

2. The Complaint charges that Defendants participated in deceptive and unfair acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. § 45(a), and deceptive and unconscionable acts and practices in violation of the UCSPA, Utah Code §§ 13-11-4 and 13-11-5, associated with their advertising, marketing, distributing, or selling pornographic content online, including videos and photos featuring child sexual abuse material ("CSAM") and non-consensual material ("NCM").

3. Defendants neither admit nor deny any of the allegations in the Complaint, except as specifically stated in this Order. Only for purposes of this action, Defendants agree not to contest jurisdiction.

4. Defendants waive any claim that they may have under the Equal Access to Justice Act, 28 U.S.C. § 2412, concerning the prosecution of this action through the date of this Order, and agree to bear their own costs and attorney fees.

5. Defendants, the Commission, and the Division waive all rights to appeal or otherwise challenge or contest the validity of this Order.

DEFINITIONS

For the purpose of this Order, the following definitions apply:

A. "Child Sexual Abuse Material" or "CSAM" means a piece of Content that depicts anyone under 18 years of age engaging in Sexually Explicit Conduct.

B. "Clear and Conspicuous" or "Clearly and Conspicuously" means that a required disclosure is easily noticeable (i.e., difficult to miss) and easily understandable by ordinary consumers, including in all of the following ways:

1. In any communication that is solely visual or solely audible, the disclosure must be made through the same means through which the communication is presented. In any communication made through both visual and audible means such as a television advertisement, the disclosure must be presented simultaneously in both the visual and audible portions of the communication even if the representation requiring the disclosure ("triggering representation") is made through only one means.
2. A visual disclosure, by its size, contrast, location, the length of time it appears, and other characteristics, must stand out from any accompanying text or other visual elements so that it is easily noticed, read, and understood.
3. An audible disclosure, including by telephone or streaming video, must be delivered in a volume, speed, and cadence sufficient for ordinary consumers to easily hear and understand it.
4. In any communication using an interactive electronic medium, such as the Internet or software, the disclosure must be unavoidable.
5. The disclosure must use diction and syntax understandable to ordinary consumers and must appear in each language in which the triggering representation appears.

6. The disclosure must comply with these requirements in each medium through which it is received, including all electronic devices and face-to-face communications.
7. The disclosure must not be contradicted or mitigated by, or inconsistent with, anything else in the communication.
8. When the representation or sales practice targets a specific audience, such as children, the elderly, or the terminally ill, "ordinary consumers" includes members of that group.

C. "Content" means any depiction of Sexually Explicit Conduct, including but not limited to a photograph, film, video, picture, audio recording, or computer-generated image.

D. "Content Partner" means any third-party entity (including its agents, employees, and affiliates) that uploads Content to a Covered Service and has certified, in writing or electronically, that the entity: 1) is duly organized, validly existing and in good standing as a corporation or other entity under the laws and regulations of the entity's jurisdiction of incorporation, organization, or chartering; 2) is subject to federal criminal recordkeeping requirements for visual depictions of actual and simulated sexually explicit conduct; and 3) owns its own website or otherwise distributes Content off of the Covered Service.

E. "Content Removal Request" means a request to remove Content from a Covered Service because it is actual or suspected CSAM and/or NCM.

F. "CRR Content" means any Content identified in a Content Removal Request by URL, title, or other information that permits Defendants to identify Content through a search of Defendants' Covered Services and internal systems.

G. "Covered Incident" means any incident that results in a Defendant notifying, pursuant to a statutory or regulatory requirement, any U.S. federal, state, or local government entity that information of or about a consumer was, or is reasonably believed to have been, accessed, acquired, or publicly exposed without authorization.

H. "Covered Information" means information from or about an individual who appears in Content on a Covered Service provided in connection with any verification of age, identification, or consent of such individual appearing in the Content, including but not limited to: (1) a first and last name; (2) a home or physical address, including street name and name of city or town; (3) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (4) a telephone number; (5) information about or derived from an individual's government-issued identification documents, such as an image of a driver's license, Social Security card, passport, or birth certificate, or the government-issued identification number associated with any such document; or (6) date of birth.

I. "Covered Service" means any website, mobile application, or online service owned or operated by a Defendant that allows third parties to upload Content for publication on such service or that republishes the same Content.

J. "Defendants" means all of the Defendants, individually, collectively, or in any combination, and their successors and assigns.

K. "Delete," "Deleted," or "Deletion," means to remove Covered Information such that it is not maintained in retrievable form and cannot be retrieved through physical or technical means.

L. "Model" means any third-party individual or entity that uploads Content to a Covered Service and is not a Content Partner.

M. "Moderator" means a human individual who reviews Content to determine whether it is or contains CSAM or NCM.

N. "Non-Consensual Material" or "NCM" means a piece of Content in which a person is engaged in Sexually Explicit Conduct without that person's consent to either the Sexually Explicit Conduct or the production, publication, disclosure, or dissemination of the Content.

O. "Sexually Explicit Conduct" means any actual or simulated sexual act, including but not limited to:

1. Sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal contact;
2. Bestiality;
3. Masturbation or any other stimulation of genitals or anus;
4. Sadistic or masochistic abuse; or
5. Lascivious exhibition of the breast(s), anus, genitals, or pubic area of any person.

P. "Suspend" or "Suspension" means to remove Content such that it is no longer available to consumers and to remove the Covered Service webpage, including all metadata, upon which the Content was hosted, and cease all monetization of the Content and Covered Service webpage.

Q. "Withdrawal of Consent" means any instance in which a person previously consented to the production and publication of Content featuring that person but a Defendant has since been informed that the person has withdrawn consent to the publication of Content.

ORDER

I. PROHIBITION AGAINST MISREPRESENTATIONS ABOUT THE PREVENTION OF POSTING AND PROLIFERATION OF CSAM AND NCM

IT IS ORDERED that Defendants, Defendants' officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, in connection with promoting or offering for sale any product or service, are permanently restrained and enjoined from misrepresenting or assisting others in misrepresenting, expressly or by implication:

A. the extent to which Defendants review and/or remove Content from Covered Services that has been flagged, or otherwise identified by anyone as CSAM, NCM, or illegal;

B. the extent to which Defendants suspend, ban, or otherwise prevent individuals or entities who have uploaded CSAM and/or NCM to any Covered Service from creating an account on, and/or uploading Content to, any Covered Service in the future;

C. the extent to which Defendants prevent CSAM or NCM that has been identified and/or removed from a Covered Service from being republished on, or otherwise made available to consumers on, any Covered Service;

D. the extent to which Defendants obtain, review, verify, or maintain paperwork required by 18 U.S.C. § 2257 for Content on a Covered Service;

E. the extent to which Defendants moderate or otherwise review Content before the Content is published or otherwise made available to a consumer on a Covered Service;

F. the extent to which any Covered Service does not contain CSAM or NCM; or

G. the extent to which Defendants prevent CSAM or NCM from being present on a Covered Service or protect consumers from the presence of CSAM or NCM on a Covered Service.

II. MANDATED SUSPENSION OF CONTENT

IT IS FURTHER ORDERED that Defendants must:

A. Within thirty (30) days after entry of this Order, indefinitely Suspend all Content uploaded by a Model to any Covered Service prior to the implementation of the CSAM and NCM Prevention Program pursuant to Provision III that Defendants have not verified that any non-Model individual participating in Sexually Explicit Conduct in the Content was eighteen (18) years of age or older at the time the Content uploaded by a Model was created, or if the creation date is unavailable, the time the Content was uploaded by a Model. *Provided, however,* such Content may be republished after Suspension if Defendants verify that any non-Model individual participating in Sexually Explicit Conduct in the Content was eighteen (18) years of age or older at the time the Content uploaded by a Model was created, or if the creation date is unavailable, the time the Content was uploaded by a Model;

B. Within three (3) months after entry of this Order, indefinitely Suspend all Content uploaded by a Model to any Covered Service prior to the implementation of the CSAM and NCM Prevention Program pursuant to Provision III that Defendants have not verified that any non-Model individual participating in Sexually Explicit Conduct in the Content consented to the Sexually Explicit Conduct, as well as to the production and publication of the Content uploaded by the Model. Such Content may be republished on the Covered Service after Suspension if Defendants verify that any non-Model individual participating in Sexually Explicit Conduct in the Content consented to the Sexually Explicit Conduct, as well as to the production and publication of Content uploaded by a Model. *Provided,*

however, that such verification is not required from a non-Model individual who has previously met the requirements set forth in Provision III.E.2.a.1-2 for other Content uploaded by the same Model; and

C. Within three (3) months after entry of this Order, indefinitely Suspend all Content uploaded by a Content Partner to any Covered Service prior to the implementation of the CSAM and NCM Prevention Program pursuant to Provision III that Defendants have not verified meets the safeguards required under sub-Provision III.E.3.a. Such Content may be republished after Suspension if Defendants verify that it meets the safeguards required under sub-Provision III.E.3.a.

Nothing in this Provision applies to Content uploaded to a Covered Service after implementation of the CSAM and NCM Prevention Program pursuant to Provision III. Such Content must meet the requirements set forth in Provision III.E.1-3.

III. MANDATED PROGRAM TO PREVENT THE POSTING AND PROLIFERATION OF CSAM AND NCM

IT IS FURTHER ORDERED that Defendants, and any business that Defendants control, in connection with making Content available on a Covered Service, must, within ninety (90) days after entry of this Order, establish and implement, and thereafter maintain, comprehensive procedures ("CSAM and NCM Prevention Program") that are designed to prevent the publication, or dissemination of, and that protects consumers from exposure to, CSAM and/or NCM on a Covered Service. To satisfy this requirement, Defendants must, at a minimum:

A. Document in writing the content, implementation, and maintenance of the CSAM and NCM Prevention Program;

B. Provide the written program and any material evaluations thereof or updates thereto to Defendants' board of directors or governing body, or, if no such board or equivalent governing body exists, to Defendants' Chief Executive Officer and Chief Operations Officer at least once every three (3) months;

C. Designate a qualified employee who reports directly to the Chief Executive Officer (or, in the event a Chief Executive Officer role does not exist, a similarly-situated executive) to coordinate and be responsible for the CSAM and NCM Prevention Program, and keep Defendants' Chief Executive Officer and board of directors or governing body informed of the CSAM and NCM Prevention Program, including all actions and procedures implemented to comply with the requirements of this Order, and any actions and procedures to be implemented to ensure continued compliance with this Order;

D. Assess and document, at least once every twelve (12) months, internal and external risks in each area of Defendants' operations that could result in CSAM or NCM being published, disseminated, or otherwise made available to a consumer on a Covered Service;

E. Design, implement, maintain, and document safeguards that control for the internal and external risks identified in response to sub-Provision III.D. Each safeguard must be based on the likelihood that the risk could be realized and result in CSAM or NCM being published, disseminated, or otherwise made available to a consumer on a Covered Service. Such safeguards must also include:

1. Policies, practices, procedures, and technical measures designed to ensure Content uploaded by a Model may not be published or otherwise made available to a consumer on a Covered Service unless Defendants:

a. Verify prior to publication (i) directly from the Model, or (ii) through documentation that establishes the age and identity of the Model as set forth by federal law, that the Model is eighteen (18) years of age or older, including authenticating that any verification documentation provided to establish the Model's age matches the Model. Defendants may only use, provide access to, or disclose any information collected for such verification to comply with the requirements set forth in Provision III; to compensate Models; to provide customer support services to Models; to communicate with Models; to maintain the functionality and security of the Covered Services; to contact or cooperate with law enforcement regarding actual or suspected CSAM, NCM, or illegal Content; or to comply with any applicable law, regulation, or court order; and

b. For each piece of Content uploaded by a Model, provide notice and a consent checkbox to the uploader of the Content to a Covered Service, which the uploader must review and endorse prior to submitting Content for review. The notice and checkbox will inform the uploader that Defendants will review Content prior to its publication and may report actual or suspected CSAM or NCM to the National Center for Missing and Exploited Children or to relevant law enforcement. The notice and consent checkbox will inform the uploader that if the Content is approved for publication it will be made public and that the uploader is waiving any privacy rights they may have previously had in the Content by submitting Content for Defendants' review;

2. Policies, practices, procedures, and technical measures designed to ensure Content uploaded by a Model is not published or otherwise made available to a consumer on a Covered Service unless Defendants:

   a. Verify prior to publication (i) directly from each non-Model individual participating in Sexually Explicit Conduct in the Content, or (ii) through documentation that establishes the age and identity of the non-Model individual as set forth by federal law, that such non-Model individual:

      1) Was eighteen (18) years of age or older at the time such Content was created, or if the creation date is unavailable, the time the Content was uploaded by a Model, including authenticating that any verification documentation provided to establish the non-Model individual's age matches the non-Model individual appearing in the Content; and

      2) Consents to the Sexually Explicit Conduct, as well as to the production and publication of the particular piece of Content. Such consent must be clearly manifested in writing or electronically.

   Such verification must rely, at least in part, on attestations or documentation submitted or otherwise provided to Defendants by the non-Model individual appearing in the Content. Defendants may only use, provide access to, or disclose any information collected for such verification to comply with the requirements set forth in Provision III; to compensate Models; to provide customer support services to Models; to communicate with Models; to maintain the functionality and security of the Covered Services; to contact or

cooperate with law enforcement regarding actual or suspected CSAM, NCM, or illegal Content; or comply with any applicable law, regulation, or court order.

Provided, however, that such verification is not required from a non-Model individual who has previously met the requirements set forth in Provision III.E.2.a.1-2 for other Content uploaded by the same Model; and

b. Unless prohibited by an applicable law, regulation, or court order, within twenty-four (24) hours of Content being published or otherwise made available to a consumer on a Covered Service, Defendants must send an e-mail or text message to the e-mail address or phone number provided for each non-Model individual appearing in Content uploaded by a Model informing the non-Model individual that Content in which they appear has been published or otherwise made available to a consumer on a Covered Service, and providing a Clear and Conspicuous link to such Content and to the Content Removal Request form pursuant to Provision III.E.9;

3. Policies, practices, procedures, and technical measures designed to ensure Content uploaded by a Content Partner must not be published or otherwise made available to a consumer on a Covered Service unless Defendants:

a. Verify prior to publication that the Content Partner certifies, in writing or electronically, that the Content Partner maintains documentation demonstrating that each individual appearing in the Content uploaded by the Content Partner: was eighteen (18) years of age or older at the time such

Content was created; and consents to the Sexually Explicit Conduct, as well as to the production and publication of the particular piece of Content;

b. Provide a notice and a consent checkbox for each piece of Content to the uploader of the Content, which the uploader must review and endorse prior to submitting Content for review. The notice and checkbox will inform the uploader that Defendants will review Content prior to its publication and may report actual or suspected CSAM or NCM to the National Center for Missing and Exploited Children or to relevant law enforcement. The notice and consent checkbox will inform the uploader that if the Content is approved for publication it will be made public and that the uploader is waving any privacy rights they may have previously had in the Content by submitting Content for Defendants' review;

4. Audit, at least once every twelve (12) months, each Content Partner with Content published or otherwise available to a consumer on a Covered Service. As part of each audit, Defendants must:

a. Request all age and consent verification documentation the Content Partner certified to maintaining for one (1) percent or twenty (20) pieces of Content, whichever quantity is greater, randomly selected by Defendants, that was published or otherwise available to a consumer on a Covered Service. *Provided, however,* after the initial audit Defendants' future audits may be limited to Content published in the last twelve (12) months;

b. Suspend the Content Partner's Content published or otherwise made available to a consumer on a Covered Service for which Content Partner fails to provide the requested age and consent verification documentation within thirty (30) days. Such Content may not be republished or otherwise made available to any consumer by Defendants unless the Content Partner provides the requested age and consent verification documentation;

c. If, as part of an audit, a Content Partner fails to provide age or consent verification documentation for any one piece of Content within forty-five (45) days, Defendants must initiate a subsequent audit pursuant to Provision III.E.4.a-c for a new sample of previously unaudited Content.

5. Utilizing available tools and technologies to review Content to determine whether it is actual or suspected CSAM or NCM prior to its publication or otherwise making it available to a consumer on a Covered Service, including, but not limited to:

a. Comparing Content, via internal or external tools, to Content previously identified and/or fingerprinted or otherwise marked (whether by any Defendant or another entity) as actual or suspected CSAM or NCM. If such a comparison indicates that a piece of Content matches previously identified or reported actual or suspected CSAM or NCM or is likely to be CSAM or NCM, and Defendants' review determines that it is likely to be actual or suspected CSAM or NCM, Defendants shall not publish it or otherwise make it available to a consumer; and

b. To the extent Defendants use Moderators to review Content:

1) At least one Moderator must exclusively watch and listen to each piece of Content in its entirety in order to make a determination about whether the Content may be CSAM or NCM. *Provided, however*, Moderators may, in lieu of listening to Content, read a complete transcript of language spoken or heard in such Content; and

2) Moderators must review the language spoken or heard in all Content. The Moderator reviewing a particular piece of Content must be either fluent in the primary languages spoken in such Content or must review a transcription of the Content that has been translated into a language in which the Moderator is fluent;

6. Mandatory CSAM and NCM prevention training that addresses the current risks and harms associated with the publication and dissemination of CSAM and NCM; any internal or external risks identified by Defendants in connection with sub-Provision III.D; and the safeguards implemented pursuant to sub-Provision III.E. This training must be provided to all Moderators and employees with responsibilities related to Content and CSAM and NCM prevention upon hire or within one hundred and twenty (120) days after entry of this Order, and on at least an annual basis thereafter.

7. Accessible methods for consumers to report possible CSAM and/or NCM to Defendants for review and removal, including but not limited to Content Removal Requests and Content flagging tools;
8. Policies, practices, procedures, and technical measures designed to ensure the consistent and thorough review of Content to determine whether it is actual or suspected CSAM or NCM, both before that Content is published on any Covered Service and upon Defendants' receipt of any report or complaint, whether by a consumer, employee, law enforcement agency, or other source (other than a person or entity known to Defendants to submit inaccurate or false reports or complaints), that the Content may be CSAM or NCM;
9. Policies, practices, procedures, and technical measures regarding Content Removal Requests, including, but not limited to:
    a. Implementing a process by which an individual, without requiring an account with a Covered Service, can submit a Content Removal Request. The process must include:
        1) A Clear and Conspicuous link or button on the home page for each Covered Service as well as each webpage displaying Content for an individual to submit a Content Removal Request;
        2) An easy-to-use Content Removal Request form that includes a Clear and Conspicuous link to an explanation of Defendants' review process;

3) Upon receipt of a Content Removal Request with an email address that Defendants have verified that the submitter has access to, the:

    a) Immediate Suspension of all Content identified in the Content Removal Request that provides a valid URL for the Content; and

    b) The Suspension, within seventy-two (72) hours of all Content identified in the Content Removal Request by title or other information that permits Defendants to identify Content through a search of Defendants' Covered Services and internal systems;

4) Upon receipt of a Content Removal Request without an email address or without an email address that Defendants have verified that the submitter has access to, the Suspension within five (5) days, of all Content identified in the Content Removal Request by URL, title, or other information that permits Defendants to identify Content through a search of Defendants' Covered Services and internal systems; and

5) Processes and technical measures that readily inform the submitter of the status of each Content Removal Request including an email address Defendants have verified that the submitter has access to submitted pursuant to this sub-provision; and

6) CRR Content may not be republished or otherwise made available to any consumer by Defendants unless Defendants confirm that the

Content meets the safeguards required under sub-Provision III.E.1-3, and that the Content is not suspected CSAM and/or NCM. For Content Removal Requests that include an email address Defendants have verified that the submitter has access to, Defendants must notify the submitter when any Content associated with the submitter's Content Removal Request is republished or otherwise made available to any consumer by Defendants;

10. Policies, practices, procedures, and technical measures regarding Withdrawal of Consent, including, but not limited to:

    a. Implementing a process by which an individual, or an individual's representative that has provided sufficient proof of representation, without being required to have an account with a Covered Service, can submit a request that Defendants remove one or more pieces of Content or all Model Content that has been verified pursuant to Provision III.E.2.a to include the individual, from Covered Service(s) based on the Withdrawal of Consent (a "Withdrawal of Consent Request"). The process must include:

        1) A Clear and Conspicuous link or button on the home page for each Covered Service as well as each webpage displaying Content or as a standalone option in the Content Removal Request process pursuant to Provision III.E.9 for an individual, or an individual's representative, to submit a Withdrawal of Consent Request, as well as a Clear and

Conspicuous link to an explanation of the process by which Defendants review each Withdrawal of Consent Request;

2) Upon receipt of a Withdrawal of Consent Request with an email address that Defendants have verified the submitter has access to:

   a) The immediate Suspension of all Content uploaded by a Model identified in a Withdrawal of Consent Request by a valid URL;

   b) The Suspension, within seventy-two (72) hours of all other instances of the same Content uploaded by a Model requested in a Withdrawal of Consent Request by a valid URL from all Covered Services;

   c) The Suspension, if requested, within seven (7) days of all Content uploaded by a Model that has been verified pursuant to Provision III.E.2.a to include the individual (collectively, "Withdrawal of Consent Model Content") from all Covered Services;

   d) Processes and technical measures that readily inform the submitter of the status of each Withdrawal of Consent Request submitted pursuant to this sub-provision;

3) Upon receipt of a Withdrawal of Consent Request without an email address that Defendants have verified the submitter has access to, the Suspension:

a) Within five (5) days, of all Content uploaded by a Model identified in the Withdrawal of Consent Request by URL, title, or other information that permits Defendants to identify Content through a search of Defendants' Covered Services and internal systems; and

b) Within ten (10) days, all other instances of the same identified Content uploaded by a Model from all Covered Services.

4) Any Content Suspended pursuant to a Withdrawal of Consent Request may only be republished or otherwise made available to a consumer by Defendants if:

a) The Withdrawal of Consent Request was submitted by an individual without sufficient proof of representation of an individual appearing in the Content uploaded by a Model;

b) Defendants confirm that the Content meets the safeguards required under sub-Provision III.E.1-2; and

c) The Content is not suspected CSAM and/or NCM;

5) For Withdrawal of Consent Requests that include an email address that Defendants have verified the submitter has access to, Defendants must notify the submitter when any Content associated with the submitter's Withdrawal of Consent Request is republished or otherwise made available to any consumer by Defendants;

b. Any Content uploaded by a Model and Suspended pursuant to Withdrawal of Consent Requests determined to have been submitted either by the individual appearing in the Content, or by a submitter with sufficient proof of representation of such individual ("Withdrawal of Consent Content"), will be subject to the following requirements:

1) Within twenty-four (24) hours of such determination, Defendants must Suspend from all Covered Services all other instances of the same Content, or portions of the same Content that Defendants are able to identify through the content identification tools and technologies utilized by Defendants in the ordinary course of business;

2) Within three (3) days of such determination, Defendants must:

a) Fingerprint or otherwise mark the Content, including all other instances of the same Content, or portions of the same Content that Defendants are able to identify through the content identification tools and technologies utilized by Defendants in the ordinary course of business, as Withdrawal of Consent Content to facilitate efforts to prevent it from being republished or otherwise made available to a consumer;

b) Delete any Covered Service webpages, including all metadata, on which the Content, including webpages where

all other instances of the same Content, or portions of the same Content that Defendants are able to identify through the content identification tools and technologies utilized by Defendants in the ordinary course of business, was hosted. *Provided, however*, that any Covered Service webpage, including all metadata, upon which the Content was hosted, that Defendants are otherwise required to Delete pursuant to this sub-provision may be retained or disclosed to the extent requested by a government agency in a formal preservation letter that identifies the specific data to be preserved or required by compulsory process, a request from law enforcement, a litigation hold, or otherwise required by law, regulation, or court order; and

c) Request that Google, Bing, and Yahoo! de-index the Covered Service webpage(s) upon which the Content was hosted. *Provided, however*, that, for search engines for which the Defendants must manually request such de-indexing, the deadline is seven (7) days after determination of the Content to be Withdrawal of Consent Content;

11. Policies, practices, procedures, and technical measures regarding registered users of a Covered Service flagging, or otherwise identifying, Content available on a

Covered Service as actual or suspected CSAM and/or NCM, including, but not limited to:

a. Implementing a process by which a registered user of a Covered Service can flag or otherwise identify Content available on a Covered Service suspected as CSAM and/or NCM. The process must include:

   1) A Clear and Conspicuous link or button in proximity to Content on each Covered Service so that any registered user may flag or otherwise identify that Content as actual or suspected CSAM and/or NCM, as well as a Clear and Conspicuous explanation of the process by which Defendants review each flag, or a Clear and Conspicuous link to such explanation;

   2) Upon receipt of a flag or other identification of Content as possible CSAM and/or NCM the Suspension, within three (3) days of Content flagged or otherwise identified as actual or suspected CSAM and/or NCM; and

   3) All Content Suspended pursuant to a flag (including all other instances of the same Content) (collectively, "Flagged Content") may not be republished or otherwise made available to any consumers by Defendants unless Defendants confirm that the Content meets the safeguards required under sub-Provision III.E.1-3, and that the Content is not suspected CSAM and/or NCM;

12. Policies, practices, procedures, and technical measures regarding requests by law enforcement agencies to remove Content available on a Covered Service because it is actual or suspected CSAM and/or NCM ("Law Enforcement Request"), including, but not limited to:

    a. Implementing a process by which any law enforcement agency can request that Defendants remove Content available on a Covered Service suspected as CSAM and/or NCM. The process must include:

        1) A Clear and Conspicuous link or button on the home page for each Covered Service so that any law enforcement agency can request the removal of Content because it is suspected as CSAM and/or NCM;

        2) Upon receipt of a Law Enforcement Request with a validated law enforcement email address:

            a) Immediate Suspension of Content identified in the Law Enforcement Request that provides a valid URL for the Content;

            b) The Suspension, within seven (7) days, of all other instances of the same Content identified by a valid URL from all Covered Services;

            c) The Suspension:

                i. Within seventy-two (72) hours, of all Content identified in the Law Enforcement Request by means other than a valid URL, such as a title or

other information that permits Defendants to identify Content through a search of Defendants' Covered Services and internal systems;

ii. Within seven (7) days, of all other instances of the same Content identified in the Law Enforcement Request by means other than a valid URL, such as a title or other information sufficient to identity the Content, from all Covered Services;

3) Processes and technical measures that readily inform a law enforcement agency of the status of each Law Enforcement Request it has submitted;

4) The Content subject to a Law Enforcement Request may not be republished or otherwise made available to any consumers by Defendants until:

a) Law enforcement that submitted the Law Enforcement Request informs Defendants that the Content is not CSAM and/or NCM; or

b) Defendants confirm the Content meets the safeguards required under sub-Provision III.E.1-3, and Defendants' review determines that it is not suspected CSAM and/or NCM, and wait forty-eight (48) hours after notifying law

enforcement that the Content will be republished or otherwise made available;

13. Policies, practices, procedures, and technical measures to address any instance in which Defendants determine that actual or suspected CSAM and/or NCM is found to be on or uploaded to a Covered Service, including, but not limited to:

    a. For instances of such actual or suspected CSAM and/or NCM identified outside the processes pursuant to sub-provisions III.E.9-12 Suspending such Content, as well as all other instances of the same Content, or portions of the same Content that Defendants are able to identify through the content identification tools and technologies utilized by Defendants in the ordinary course of business, from all Covered Services within twenty-four (24) hours of Defendants' review determining that it is actual or suspected CSAM and/or NCM;

    b. Within three (3) days of determination of such Content to be actual or suspected CSAM and/or NCM:

        1) Fingerprinting or otherwise marking the Content, including all other instances of the same Content, as actual or suspected CSAM and/or NCM to facilitate efforts to prevent it from being republished or otherwise made available to a consumer;

        2) Deleting any Covered Service webpages, including all metadata, on which the Content, including webpages where all other instances of the same or Content, or portions of the same Content

that Defendants are able to identify through the content identification tools and technologies utilized by Defendants in the ordinary course of business, was hosted. *Provided, however*, that any Covered Service webpage, including all metadata, upon which the Content was hosted, that Defendants are otherwise required to Delete pursuant to this sub-provision may be retained or disclosed to the extent requested by a government agency in a formal preservation letter that identifies the specific data to be preserved or required by compulsory process, a request from law enforcement, a litigation hold, or otherwise required by law, regulation, or court order; and

3) Requesting that Google, Bing, and Yahoo! de-index the Covered Service webpage(s) upon which the Content was hosted. *Provided, however*, that, for search engines for which the Defendants must manually request such de-indexing, the deadline is seven (7) days after Defendants' review determines that the Content it is actual or suspected CSAM and/or NCM;

c. For Content uploaded by a Model determined to be such actual or suspected CSAM and/or NCM within seven (7) days, Defendants must:

1) Suspend all Content on all Covered Services uploaded by the Model who uploaded the CSAM and/or NCM Content;

2) Ban all accounts of that Model from all Covered Services, and implement measures to facilitate efforts to prevent the Model from creating an account for uploading Content to, any Covered Service; and

d. Within seven (7) days of determination of actual or suspected CSAM and/or NCM Content, upon request of any non-consenting individuals featured in such Content, assigning a case manager responsible for responding to information requests or other inquiries from the individual relating to such Content;

14. Policies, practices, procedures, and technical measures to address instances where Defendants determine that – pursuant to a Content Removal Request(s) and/or Withdrawal of Consent Request(s) – one (1) percent or more of the Content uploaded by a Content Partner and published on a Covered Service is actual or suspected CSAM and/or NCM:

a. Within sixty (60) days of Defendants' determination that one (1) percent or more of the Content uploaded by a Content Partner and published on a Covered Service is actual or suspected CSAM and/or NCM, conduct and complete an audit of the Content Partner's age and consent verification. Such audit cannot be based solely on a review of the Content Partner's age and consent verification documentation. *Provided, however*, nothing shall prevent Defendants from banning all accounts, and Deleting all Content on all

Covered Services of a Content Partner at any time, including prior to completion of such audit;

b. If pursuant to such audit Defendants are unable to confirm the age and consent for ten (10) percent or more of the Content uploaded by the Content Partner and published on a Covered Service, then Defendants must:

1) Suspend all Content of the Content Partner on all Covered Services; and

2) Ban all accounts of that Content Partner from all Covered Services and implement measures to facilitate efforts to prevent the Content Partner from creating an account for uploading Content to, any Covered Service;

15. Policies, practices, procedures, and technical measures so that a registered user of a Covered Service can flag or otherwise report to Defendants for review a user comment or direct message between users on a Covered Service, to the extent available, because the comment or message (a) promotes, encourages, or solicits the creation, publication, or dissemination of CSAM and/or NCM, or (b) encourages, promotes, solicits, or engages in child abuse or non-consensual sexual activities. The process must include:

a. A Clear and Conspicuous link or button in proximity to each user comment and direct message between users so that a registered user may flag or otherwise report the comment or direct message for review by Defendants, as

well a Clear and Conspicuous link to an explanation of the process by which Defendants review each flag or report;

b. Defendants' review of any flagged or otherwise reported user comment or direct message within three (3) days of such flagging or reporting to determine whether it (i) promotes, encourages, or solicits the creation, publication, or dissemination of CSAM and/or NCM, or (ii) encourages, promotes, solicits, or engages in child abuse or non-consensual sexual activities;

c. The immediate removal of any user comment or direct message Defendants determine (i) promotes, encourages, or solicits the creation, publication, or dissemination of CSAM and/or NCM, or (ii) encourages, promotes, solicits, or engages in child abuse or non-consensual sexual activities; and

d. The banning, within three (3) days, of any registered user that Defendants determine has posted a comment or sent a direct message (i) promoting, encouraging, or soliciting the creation, publication, or dissemination of CSAM and/or NCM, or (ii) encouraging, promoting, soliciting, or engaging in child abuse or non-consensual sexual activities. In banning such a registered user, Defendants must ban all accounts of that user on all Covered Services and implement measures to facilitate efforts to prevent the user from creating an account for uploading Content to, any Covered Service;

16. Policies, practices, procedures, and technical measures to deter persons from searching for or tagging or titling Content on a Covered Service with terms

Defendants have determined suggest the Content is CSAM and/or NCM, including but not limited to:

a. Displaying a message whenever a person searches for Content using such terms:

   1) Stating that the person may be attempting to access Content that is CSAM and/or NCM, which may be illegal; and

   2) Where available, providing contact information for organizations that provide help to persons who have sought CSAM and/or NCM; and

b. Preventing uploaders from tagging or titling Content on any Covered Service with such terms;

17. To the extent Defendants review Content using Moderators, policies, practices, and procedures designed to ensure that Moderators effectively identify and remove CSAM and NCM, including, but not limited to:

    a. Providing mandatory training for Moderators as to the identification and detection of CSAM and NCM, upon hire and at least every twelve (12) months thereafter; and

    b. Prohibiting a Moderator's salary, bonus, or any other financial compensation from being based solely on the amount or quantity of Content that the Moderator reviews during any given time period; and

18. Policies, practices, procedures, and technical measures designed to ensure Defendants report any actual or suspected CSAM uploaded to, or identified on, a Covered Service to the National Center for Missing and Exploited Children

within seventy-two (72) hours of Defendants' determination that the Content is actual or suspected CSAM;

F. At least once every twelve (12) months:

1. Assess the sufficiency of any safeguards in place to address the internal and external risks that could result in the publication of CSAM or NCM on a Covered Service, and modify the CSAM and NCM Prevention Program based on the results; and
2. Monitor the effectiveness of the safeguards and modify the CSAM and NCM Prevention Program based on the results;

G. Evaluate and adjust the CSAM and NCM Prevention Program in light of any material changes to:

1. Defendants' operations or business arrangements;
2. New or more efficient technological or operational methods to control for the risks identified in Provision III.D of this Order; or
3. Any other circumstances that Defendants know or have reason to know may have a material impact on the effectiveness of the CSAM and NCM Prevention Program or any of its individual safeguards;

At a minimum, Defendants must evaluate the CSAM and NCM Prevention Program at least once every twelve (12) months and modify the CSAM and NCM Prevention Program based on the results; and

H. Within ninety (90) days of June 30 and December 31 of each calendar year, publish a hyperlink on the home page of each Covered Service to a report detailing, using diction and

syntax understandable to reasonable consumers, Defendants' implementation and enforcement of policies, practices, procedures, and technical measures to prevent the publication, and dissemination of CSAM and NCM on such Covered Services ("CSAM and NCM Prevention Transparency Report"). Each CSAM and NCM Prevention Transparency Report must include the following information for the six (6) months preceding the end of the applicable reporting period (i.e., June 30, December 31):

1. A description of all business units or teams (e.g., compliance, Moderators) involved in Defendants' CSAM and NCM prevention efforts;
2. A description of each policy, practice, process, procedure, tool, and technical measure employed by Defendants designed to ensure that the Covered Services are not used for the publication or dissemination of CSAM and/or NCM, including but not limited to:
    a. A description of each policy, practice, process, procedure, tool, and technical measure employed by Defendants to verify the identity, age, and consent of each person depicted participating in the Sexually Explicit Conduct in Content on the Covered Services;
    b. A description of what constitutes CSAM and NCM;
    c. A description of each policy, practice, procedure, tool, and technical measure employed by Defendants to detect, identify, remove, and/or report CSAM and NCM;
    d. A graphical representation of the process by which Defendants review Content for the presence of CSAM and NCM;

e. A description of the review process where a Moderator does not speak the language spoken or presented in Content;

f. A description of Defendants' processes for responding to CSAM and NCM on the Covered Services, including but not limited to those concerning persons and entities attempting to upload CSAM or NCM to a Covered Service or otherwise using a Covered Service to disseminate CSAM or NCM;

g. A description of each process by which consumers, organizations, and law enforcement agencies may report or flag actual or suspected CSAM and NCM on the Covered Services to Defendants, as well as the policies, practices, and procedures governing Defendants' response to any such report or flag;

h. A description of all processes by which, and categories of circumstances under which, Defendants report CSAM and NCM to an external organization or agency;

i. A description of Defendants' membership in any industry organizations, partnerships, or other collaborations related to the detection, identification, removal, and/or prevention of CSAM or NCM, or related to child safety; and

j. An explanation of any material updates or changes to Defendants' policies, practices, procedures, or technical measures insofar as they relate

to preventing the upload of, or to the detection, identification, and/or removal of CSAM or NCM; and

3. Detailed metrics on the results of Defendants' efforts designed to ensure that the Covered Services are not used for the publication or dissemination of CSAM and/or NCM, including both narrative explanation and numerical data displayed in charts and/or graphs on the following metrics:

    a. The number of photos and videos uploaded to the Covered Services;

    b. The number of photos and videos published or otherwise made available to a consumer on the Covered Services;

    c. The number of unique Withdrawal of Consent Requests received in connection with the Covered Services;

    d. The number of unique Content Removal Requests, flags, and Law Enforcement Requests received in connection with actual or suspected CSAM or NCM on the Covered Services;

    e. The number of actual or suspected CSAM and NCM photos and videos uploaded to, but not published or otherwise made available to consumers on, the Covered Services, including a breakdown of how such Content was identified as actual or suspected CSAM or NCM (e.g., moderation, tool, technology);

    f. The number of actual or suspected CSAM and NCM photos and videos removed from the Covered Services, including a breakdown of how such Content was identified as actual or suspected CSAM or NCM (e.g.,

moderation, technology, Content Removal Request, flag, Law Enforcement Request), the average number of days such Content was available on the Covered Services, and the average number of views such Content received before it was removed;

g. The number of accounts identified as attempting to upload, publish, or disseminate actual or suspected CSAM and/or NCM in connection with the Covered Services, as well as a breakdown of what actions were taken with respect to these accounts in response;

h. The number of accounts suspended, banned, or otherwise actioned in connection with the attempted upload, publication, or dissemination of actual or suspected CSAM and/or NCM in connection with the Covered Services, as well as how many of these accounts were reinstated and the reasons for any such reinstatements; and

i. The number of reports of actual or suspected CSAM and NCM made to outside organizations that seek to prevent CSAM or NCM (e.g., the National Center for Missing and Exploited Children).

IV. CSAM AND NCM PREVENTION PROGRAM ASSESSMENTS BY A THIRD PARTY

IT IS FURTHER ORDERED that, in connection with compliance with Provision III of this Order titled Mandated Program to Prevent the Posting and Proliferation of CSAM and NCM,

Defendants must obtain initial and biennial assessments ("CSAM and NCM Prevention Assessment(s)"):

A. The CSAM and NCM Prevention Assessments must be obtained from one or more qualified, objective, independent third-party professionals ("CSAM and NCM Prevention Assessor"), who: (1) use procedures and standards generally accepted in the profession; (2) conduct an independent review of the CSAM and NCM Prevention Program; (3) retain all documents relevant to each CSAM and NCM Prevention Assessment for five (5) years after completion of such CSAM and NCM Prevention Assessment; and (4) will provide such documents to the Commission and the Division within ten (10) days of receipt of a written request from a representative of the Commission. No documents may be withheld from the Commission or the Division by the CSAM and NCM Prevention Assessor on the basis of a claim of confidentiality, proprietary or trade secrets, work product protection, attorney-client privilege, statutory exception, or any similar claim.

B. For each CSAM and NCM Prevention Assessment, Defendants must provide the Associate Director for Enforcement for the Bureau of Consumer Protection at the Federal Trade Commission with the name, affiliation, and qualifications of the proposed CSAM and NCM Prevention Assessor, whom the Associate Director shall have the authority to approve in her or his sole discretion.

C. The reporting period for the CSAM and NCM Prevention Assessments must cover: (1) the first one hundred eighty (180) days after the entry date of this Order for the initial CSAM and NCM Prevention Assessment; and (2) each two (2)-year period thereafter for ten (10) years after entry of this Order for the biennial CSAM and NCM Prevention Assessments.

D. Each CSAM and NCM Prevention Assessment must, for the entire assessment period: (1) determine whether Defendants have implemented and maintained the CSAM and NCM Prevention Program required by Provision III of this Order, titled Mandated Program to Prevent the Posting and Proliferation of CSAM and NCM; (2) assess the effectiveness of Defendants' implementation and maintenance of sub-Provisions III.A-H; (3) identify any gaps or weaknesses in, or instances of material noncompliance with, the CSAM and NCM Prevention Program; (4) address the status of gaps or weaknesses in, or instances of material non-compliance with the CSAM and NCM Prevention Program that were identified in any prior CSAM and NCM Prevention Assessment required by this Order; (5) identify specific evidence (including documents reviewed, sampling and testing performed, and interviews conducted) examined to make such determinations, assessments, and identifications, and explain why the evidence that the CSAM and NCM Prevention Assessor examined is (a) appropriate for assessing an enterprise of Defendants' size, complexity, and risk profile; and (b) sufficient to justify the CSAM and NCM Prevention Assessor's findings. No findings of any CSAM and NCM Prevention Assessment shall rely primarily on assertions or attestations by Defendants' management. The CSAM and NCM Prevention Assessment must be signed by the CSAM and NCM Prevention Assessor, state that the CSAM and NCM Prevention Assessor conducted an independent review of the CSAM and NCM Prevention Program and did not rely primarily on assertions or attestations by Defendants' management, and state the number of hours that each member of the assessment team worked on the CSAM and NCM Prevention Assessment. To the extent that Defendants materially revise or update or add one or more safeguards required under Provision III of this Order during a CSAM and NCM Prevention Assessment period, the CSAM and NCM

Prevention Assessment must assess the effectiveness of the revised, updated, or added safeguard(s) for the time period in which it was in effect, and provide a separate statement detailing the basis for each revised, updated, or additional safeguard.

E. Each CSAM and NCM Prevention Assessment must be completed within ninety (90) days after the end of the reporting period to which the CSAM and NCM Prevention Assessment applies. Unless otherwise directed by the Associate Director for Enforcement for the Bureau of Consumer Protection at the Federal Trade Commission in writing, Defendants must submit the initial CSAM and NCM Prevention Assessment to the Commission and the Division within fourteen (14) days after the CSAM and NCM Prevention Assessment has been completed via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580, and via email to WCCE@agutah.gov or by overnight courier (not the U.S. Postal Service) to the Utah Attorney General's Office, White Collar and Commercial Enforcement Division, 160 East 300 South, 5th Floor, Salt Lake City, UT 84114. The subject line must begin, "FTC v. MindGeek, FTC File No. 2123033." All subsequent biennial CSAM and NCM Prevention Assessments must be retained by Defendants until the Order is terminated and provided to the Associate Director for Enforcement within ten (10) days of request. The initial CSAM and NCM Prevention Assessment and any subsequent biennial CSAM and NCM Prevention Assessment provided to the Commission and the Division must be marked, in the upper right-hand corner of each page, with the words "DPIP CSAM and NCM Prevention Assessment" in red lettering.

V. COOPERATION WITH THIRD-PARTY CSAM AND NCM PREVENTION ASSESSOR

IT IS FURTHER ORDERED that Defendants, whether acting directly or indirectly, in connection with any Prevention Assessment required by Provision IV of this Order titled Prevention Assessments by a Third Party, must:

A. Provide or otherwise make available to the CSAM and NCM Prevention Assessor all information and material in their possession, custody, or control that is relevant to the CSAM and NCM Prevention Assessment for which there is no reasonable claim of privilege;

B. Provide or otherwise make available to the CSAM and NCM Prevention Assessor Defendants' content management system(s) and customer support network(s); and

C. Disclose all material facts to the CSAM and NCM Prevention Assessor, and not misrepresent in any manner, expressly or by implication, any fact material to the CSAM and NCM Prevention Assessor's: (1) determination of whether Defendants have implemented and maintained the CSAM and NCM Prevention Program; (2) assessment of the effectiveness of the implementation and maintenance of sub-Provisions III.A–H; or (3) identification of any gaps or weaknesses in, or instances of material noncompliance with, the CSAM and NCM Prevention Program.

VI. ANNUAL CERTIFICATIONS – CSAM AND NCM PREVENTION

IT IS FURTHER ORDERED that Defendants must:

A. One year after the entry date of this Order, and each year thereafter, provide the Commission and the Division with a certification from the Chief Executive Officer that: (1) Defendants have established, implemented, and maintained the requirements under Provisions I–V of this Order; and (2) Defendants are not aware of any material noncompliance that has not

been (a) corrected or (b) disclosed to the Commission and the Division. The certification must be based on the personal knowledge of the Chief Executive Officer or subject matter experts upon whom the Chief Executive Officer relies in making the certification.

B. Unless otherwise directed by a Commission representative in writing, submit all CSAM and NCM Prevention annual certifications to the Commission and the Division pursuant to this Order via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580, and via email to WCCE@agutah.gov or by overnight courier (not the U.S. Postal Service) to the Utah Attorney General's Office, White Collar and Commercial Enforcement Division, 160 East 300 South, 5th Floor, Salt Lake City, UT 84114. The subject line must begin: "FTC v. MindGeek, FTC File No. 2123033."

VII. NOTICE TO USERS

IT IS FURTHER ORDERED that on or before fourteen (14) days after the entry date of this Order, Defendants must post Clearly and Conspicuously on the landing pages for each Covered Service, a link to an exact copy of the notice attached hereto as Exhibit A ("Notice"). Defendants must leave this Notice in place for two (2) years after posting it.

VIII. PROHIBITION AGAINST MISREPRESENTATIONS ABOUT PRIVACY OR INFORMATION SECURITY

IT IS FURTHER ORDERED that Defendants, Defendants' officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, in connection with

promoting or offering for sale any product or service, are permanently restrained and enjoined from misrepresenting or assisting others in misrepresenting, expressly or by implication:

A. The extent to which Defendants collect, maintain, use, disclose, Delete, or permit or deny access to any Covered Information;

B. The purpose(s) for which Defendants collect, maintain, use, disclose, or permit access to any Covered Information;

C. The extent to which Models, Content Partners, or any other individual who submits age or consent verification documentation to Defendants may exercise control over Defendants' collection of, maintenance of, use of, Deletion of, disclosure of, or permission of access to, Covered Information, and the steps a Model, Content Partner, or any other individual who submits age or consent verification documentation to Defendants must take to implement such controls; or

D. The extent to which Defendants protect the privacy, security, availability, confidentiality, or integrity of any Covered Information.

IX. MANDATED PRIVACY AND INFORMATION SECURITY PROGRAM

IT IS FURTHER ORDERED that Defendants and any business that Defendants control, directly or indirectly, in connection with the collection, maintenance, use, or disclosure of, or provision of access to, Covered Information, must, within sixty (60) days after entry of this Order, establish and implement, and thereafter maintain, a comprehensive privacy and information security program ("Privacy and Information Security Program") that protects the privacy, security, availability, confidentiality, and integrity of Covered Information. To satisfy this requirement, Defendants must, at a minimum:

A. Document in writing the relevant content, implementation, and maintenance of the Privacy and Information Security Program;

B. Provide the written program and any evaluations thereof or material updates thereto to Defendants' board of directors or governing body or, if no such board or equivalent governing body exists, to a senior officer of Defendants responsible for the Privacy and Information Security Program at least once every twelve (12) months and promptly (not to exceed sixty (60) days) after discovery of a Covered Incident;

C. Designate a qualified employee or employees, who report(s) directly to an executive, such as the Chief Executive Officer or Chief Operations Officer, to coordinate and be responsible for the Privacy and Information Security Program; and keep the executive and the board of directors informed of the Privacy and Information Security Program, including all actions and procedures implemented to comply with the requirements of this Order, and any actions and procedures to be implemented to ensure continued compliance with this Order;

D. Assess and document, at least once every twelve (12) months and promptly (not to exceed thirty (30) days) following discovery of a Covered Incident, internal and external risks to the privacy, security, availability, confidentiality, or integrity of Covered Information that could result in the (1) unauthorized collection, maintenance, alteration, use, Deletion, disclosure of, or provision of access to, Covered Information; or (2) misuse, loss, theft, alteration, destruction, or other compromise of Covered Information;

E. Design, implement, maintain, and document safeguards that control for the internal and external risks Defendants identify to the privacy, security, availability, confidentiality, or integrity of Covered Information identified in response to sub-Provision IX.D. Each safeguard

must be based on the volume and sensitivity of the Covered Information that is at risk, and the likelihood that the risk could be realized and result in the (1) unauthorized collection, maintenance, alteration, use, Deletion, disclosure of, or provision of access to, the Covered Information; or the (2) misuse, loss, theft, alteration, destruction, or other compromise of the Covered Information. Such safeguards must also include:

1. Policies, practices, procedures, and technical measures to systematically inventory Covered Information in Defendants' control. *Provided, however*, that any Covered Information that Defendants are otherwise required to Delete pursuant to this sub-provision may be retained or disclosed to the extent requested by a government agency in a formal preservation letter that identifies the specific data to be preserved or required by compulsory process, a request from law enforcement, a litigation hold, or otherwise required by law, regulation, or court order;
2. Data access controls for all assets (including databases) containing Covered Information, including but not limited to:
    a. Limiting employee access to Covered Information by, at a minimum, limiting employee access to what is needed to perform that employee's job function;
    b. Granting and auditing varying levels of access based on an employee's need to know; and
    c. Requiring multi-factor authentication methods for all employees in order to access any assets (including databases) storing Covered Information. Such

multi-factor authentication methods shall not include telephone or SMS-based authentication methods and must be resistant to phishing attacks;

3. Policies, practices, procedures, and technical measures to segment, or otherwise keep separate, Covered Information from Content;
4. Encryption, or at least equivalent protection, of all Covered Information in Defendants' control that is reasonably linkable to a consumer, computer, or device, including in transit and at rest;
5. Technical, organizational, and as appropriate, physical controls to safeguard against unauthorized access to any asset (including databases) containing Covered Information in Defendants' control, such as properly configured firewalls;
6. A data retention policy that, at a minimum, includes:
   a. A requirement that Defendants document, adhere to, and make publicly available on Defendants' terms of service/use a retention schedule for Covered Information, setting forth: (1) the purposes for which the Covered Information is collected; (2) the specific business need for retaining each type of Covered Information; and (3) a specific timeframe for Deletion of each type of Covered Information (absent any intervening Deletion requests from individuals);
7. Policies, practices, procedures, and technical measures designed to ensure that Covered Information collected for verification or consent purposes, such as pursuant to Provision III of this Order, is not used for any other purpose or disclosed to a third party. *Provided, however*, the Covered Information collected

for verification or consent purposes may be used for the purpose of complying with the requirements set forth in Provision III; to compensate Models; to provide customer support services to Models; to communicate with Models; to maintain the functionality and security of the Covered Services; to contact or cooperate with law enforcement regarding actual or suspected CSAM, NCM, or illegal Content; or to comply with any applicable law, regulation, or court order; and

8. Training of all of Defendants' employees upon hire or within one hundred and twenty (120) days after entry of this Order, and at least once every twelve (12) months for employees with access to Covered Information, on how to safeguard Covered Information;

F. Assess, at least once every twelve (12) months and promptly (not to exceed thirty (30) days) following discovery of a Covered Incident, the sufficiency of any safeguards in place to address the internal and external risks to the privacy, security, availability, confidentiality, or integrity of Covered Information, and modify the Privacy and Information Security Program based on the results;

G. Test and monitor the effectiveness of the safeguards at least once every twelve (12) months and promptly (not to exceed thirty (30) days) following discovery of a Covered Incident, and modify the Privacy and Information Security Program based on the results. Such testing and monitoring must include vulnerability testing of Defendants' network(s) once every four (4) months and promptly (not to exceed thirty (30) days) after discovery of a Covered Incident, and penetration testing of Defendants' network(s) at least once every twelve (12) months and promptly (not to exceed thirty (30) days) after a Covered Incident;

H. Select and retain service providers capable of safeguarding Covered Information they access through or receive from Defendants, and contractually require service providers to implement and maintain safeguards sufficient to address the internal and external risks to the privacy, security, availability, confidentiality, or integrity of Covered Information; and

I. Evaluate and adjust the Privacy and Information Security Program in light of any changes to Defendants' operations or business arrangements, a Covered Incident, new or more efficient technological or operational methods to control for the risks identified in Provision IX.D of this Order, or any other circumstances that Defendants know or have reason to know may have a material impact on the effectiveness of the Privacy and Information Security Program or any of its individual safeguards. At a minimum, Defendants must evaluate the Privacy and Information Security Program at least once every twelve (12) months and modify the Privacy and Information Security Program based on the results.

X. PRIVACY AND INFORMATION SECURITY ASSESSMENTS BY A THIRD PARTY

IT IS FURTHER ORDERED that, in connection with compliance with Provision IX of this Order titled Mandated Privacy and Information Security Program, Defendants must obtain initial and biennial assessments ("Privacy and Security Assessment(s)"):

A. The Privacy and Security Assessments must be obtained from one or more qualified, objective, independent third-party professionals ("Privacy and Security Assessor"), who: (1) use procedures and standards generally accepted in the profession; (2) conduct an independent review of the Privacy and Information Security Program; (3) retain all documents relevant to each Privacy and Security Assessment for five (5) years after completion of such Privacy and Security Assessment; and (4) will provide such documents to the Commission and the Division

within ten (10) days of receipt of a written request from a representative of the Commission. No documents may be withheld from the Commission or the Division by the Privacy and Security Assessor on the basis of a claim of confidentiality, proprietary or trade secrets, work product protection, attorney-client privilege, statutory exception, or any similar claim.

B. For each Privacy and Security Assessment, Defendants must provide the Associate Director for Enforcement for the Bureau of Consumer Protection at the Federal Trade Commission with the name, affiliation, and qualifications of the proposed Privacy and Security Assessor, whom the Associate Director shall have the authority to approve in her or his sole discretion.

C. The reporting period for the Privacy and Security Assessments must cover: (1) the first one hundred eighty (180) days after the entry date of this Order for the initial Privacy and Security Assessment; and (2) each two (2) year period thereafter for ten (10) years after entry of this Order for the biennial Privacy and Security Assessments.

D. Each Privacy and Security Assessment must, for the entire assessment period: (1) determine whether Defendants have implemented and maintained the Privacy and Information Security Program required by Provision IX of this Order, titled Mandated Privacy and Information Security Program; (2) assess the effectiveness of Defendants' implementation and maintenance of sub-Provisions IX.A-I; (3) identify any gaps or weaknesses in, or instances of material noncompliance with, the Privacy and Information Security Program; (4) address the status of gaps or weaknesses in, or instances of material non-compliance with the Privacy and Information Security Program that were identified in any prior Privacy and Security Assessment required by this Order; (5) identify specific evidence (including documents reviewed, sampling

and testing performed, and interviews conducted) examined to make such determinations, assessments, and identifications, and explain why the evidence that the Privacy and Security Assessor examined is (a) appropriate for assessing an enterprise of Defendants' size, complexity, and risk profile; and (b) sufficient to justify the Privacy and Security Assessor's findings. No findings of any Privacy and Security Assessment shall rely primarily on assertions or attestations by Defendants' management. The Privacy and Security Assessment must be signed by the Privacy and Security Assessor, state that the Privacy and Security Assessor conducted an independent review of the Privacy and Information Security Program and did not rely primarily on assertions or attestations by Defendants' management, and state the number of hours that each member of the assessment team worked on the Privacy and Security Assessment. To the extent that Defendants materially revise or update or add one or more safeguards required under Provision IX of this Order during a Privacy and Security Assessment period, the Privacy and Security Assessment must assess the effectiveness of the revised, updated, or added safeguard(s) for the time period in which it was in effect, and provide a separate statement detailing the basis for each revised, updated, or additional safeguard.

E. Each Privacy and Security Assessment must be completed within sixty (60) days after the end of the reporting period to which the Privacy and Security Assessment applies. Unless otherwise directed by a Commission representative in writing, Defendants must submit the initial Privacy and Security Assessment to the Commission and the Division within fourteen (14) days after the Privacy and Security Assessment has been completed via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW,

Washington, DC 20580, and via email to WCCE@agutah.gov or by overnight courier (not the U.S. Postal Service) to the Utah Attorney General's Office, White Collar and Commercial Enforcement Division, 160 East 300 South, 5th Floor, Salt Lake City, UT 84114. The subject line must begin, "FTC v. MindGeek, FTC File No. 2123033." All subsequent biennial Privacy and Security Assessments must be retained by Defendants until the Order is terminated and provided to the Associate Director for Enforcement within ten (10) days of request. The initial Privacy and Security Assessment and any subsequent biennial Privacy and Security Assessment provided to the Commission and the Division must be marked, in the upper right-hand corner of each page, with the words "DPIP Privacy and Security Assessment" in red lettering.

XI. COOPERATION WITH THIRD-PARTY PRIVACY AND INFORMATION SECURITY ASSESSOR

IT IS FURTHER ORDERED that Defendants, whether acting directly or indirectly, in connection with any Privacy and Security Assessment required by Provision X of this Order titled Privacy and Security Assessments by a Third Party, must:

A. Provide or otherwise make available to the Privacy and Security Assessor all information and material in its possession, custody, or control that is relevant to the Privacy and Security Assessment for which there is no reasonable claim of privilege;

B. Provide or otherwise make available to the Privacy and Security Assessor information about Defendants' network(s) and all of Defendants' IT assets so that the Privacy and Security Assessor can determine the scope of the Privacy and Security Assessment, and visibility to those portions of the network(s) and IT assets deemed in scope; and

C. Disclose all material facts to the Privacy and Security Assessor, and not misrepresent in any manner, expressly or by implication, any fact material to the Privacy and Security

Assessor's: (1) determination of whether Defendants have implemented and maintained the Privacy and Information Security Program; (2) assessment of the effectiveness of the implementation and maintenance of sub-Provisions IX.A-I; or (3) identification of any gaps or weaknesses in, or instances of material noncompliance with, the Privacy and Information Security Program.

XII. ANNUAL CERTIFICATIONS – PRIVACY AND INFORMATION SECURITY

IT IS FURTHER ORDERED that Defendants must:

A. One year after the entry date of this Order, and each year thereafter, provide the Commission and the Division with a certification from the senior corporate manager, or, if no such senior corporate manager exists, a senior officer of Defendants responsible for Defendants' Privacy and Information Security Program that: (1) Defendants have established, implemented, and maintained the requirements of this Order; (2) Defendants are not aware of any material noncompliance that has not been (a) corrected or (b) disclosed to the Commission and the Division; and (3) includes a brief description of all Covered Incidents during the certified period. The certification must be based on the personal knowledge of a senior corporate manager, or, if no such senior corporate manager exists, a senior officer of Defendants responsible for Defendants' Privacy and Information Security Program, or subject matter experts upon whom the senior corporate manager, or, if no such senior corporate manager exists, a senior officer of Defendants responsible for Defendants' Privacy and Information Security Program, reasonably relies in making the certification.

B. Unless otherwise directed by a Commission representative in writing, submit all privacy and information security annual certifications to the Commission pursuant to this Order via email

to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580, and via email to WCCE@agutah.gov or by overnight courier (not the U.S. Postal Service) to the Utah Attorney General's Office, White Collar and Commercial Enforcement Division, 160 East 300 South, 5th Floor, Salt Lake City, UT 84114. The subject line must begin: "FTC v. MindGeek, FTC File No. 2123033."

XIII. COVERED INCIDENT REPORTS

IT IS FURTHER ORDERED that, within ten (10) days of any notification to a United States federal, state, or local entity of a Covered Incident, Defendants shall submit a report to the Commission and the Division. The report must include, to the extent possible:

A. The date, estimated date, or estimated date range when the Covered Incident occurred;

B. A description of the facts relating to the Covered Incident, including the causes of the Covered Incident, if known;

C. A description of each type of information that was affected by the Covered Incident;

D. The number of consumers whose information was affected by the Covered Incident;

E. The acts that Defendants have taken to date to remediate the Covered Incident and protect Covered Information from further exposure or access, and protect affected individuals from identity theft or other harm that may result from the Covered Incident; and

F. A representative copy of each materially different notice sent by Defendants to individuals or to any U.S. federal, state, or local government entity.

G. Unless otherwise directed by a Commission representative in writing, all Covered Incident reports pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight

courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580, and via email to WCCE@agutah.gov or by overnight courier (not the U.S. Postal Service) to the Utah Attorney General's Office, White Collar and Commercial Enforcement Division, 160 East 300 South, 5th Floor, Salt Lake City, UT 84114. The subject line must begin: "FTC v. MindGeek, FTC File No. 2123033."

XIV. MONETARY JUDGMENT

IT IS FURTHER ORDERED that:

A. Judgment in the amount of fifteen million dollars ($15,000,000) is entered in favor of the Division against Defendants, jointly and severally, as civil penalties.

B. The Defendants are ordered to pay the Division five million dollars ($5,000,000) by electronic fund transfer within seven (7) days of entry of this Order.

C. The Division agrees to suspend the remaining ten million dollars ($10,000,000) of the judgment conditional on each Defendant complying with the Provisions of this Order.

D. The Division may revoke the suspension of the remaining judgment only if (1) the Division informs Defendants in writing that the Division believes a Provision of this Order has been violated, identifying the specific Provision and conduct that the Division believes gives rise to the violation and how the violation can be reasonably cured ("Notice of Potential Violation"); (2) Defendants do not cure the violation identified in the Notice of Potential Violation within sixty (60) days of receiving the Notice of Potential Violation; and (3) the Division then moves for a contempt order and the court finds any Defendant in contempt of this Order based, at least

in part, on a finding that the Defendant violated the Provision of this Order as identified in the Notice of Potential Violation and that contempt finding is no longer subject to appeal.

E. If the above conditions are met, the Division may revoke the suspension of the remaining judgment by sending written notice to the Defendants ("Notice of Suspension Revocation"). After receipt of the Notice of Suspension Revocation, Defendants must pay to the Division the full amount of the remaining judgment within thirty (30) days, for which all Defendants are jointly and severally liable.

F. Nothing in this Provision affects the Commission's rights to investigate or monitor compliance with this Order; and nothing requires the Commission to give prior notice to Defendants before or while investigating or monitoring compliance or before seeking any contempt remedy.

XV. ADDITIONAL MONETARY PROVISIONS

IT IS FURTHER ORDERED that:

A. The Defendants relinquish dominion and all legal and equitable right, title, and interest in all assets transferred pursuant to this Order and may not seek the return of any assets.

B. The facts alleged in the Complaint will be taken as true, without further proof, in any subsequent civil litigation by or on behalf of the Plaintiffs to enforce the Plaintiffs' rights to any payment or monetary judgment pursuant to this Order, such as a nondischargeable complaint in any bankruptcy case.

C. The facts alleged in the Complaint establish all elements necessary to sustain an action by the Plaintiffs pursuant to Section 523(a)(2)(A) of the Bankruptcy Code, 11 U.S.C. § 523(a)(2)(A), and this Order will have collateral estoppel effect for such purposes.

D. The Defendants acknowledge that their Tax Identification Numbers, which the Defendants must submit to the Plaintiffs, may be used for collecting and reporting on any delinquent amount arising out of this Order, in accordance with 31 U.S.C. § 7701.

XVI. ORDER ACKNOWLEDGMENTS

IT IS FURTHER ORDERED that Defendants obtain acknowledgments of receipt of this Order:

A. Each Defendant, within seven (7) days of entry of this Order, must submit to the Commission and the Division an acknowledgment of receipt of this Order sworn under penalty of perjury.

B. For ten (10) years after entry of this Order, each Defendant must deliver a copy of this Order to: (1) all principals, officers, directors, and LLC managers and members; (2) all employees, agents, and representatives having managerial responsibilities for conduct related to the subject matter of the Order; and (3) any business entity resulting from any change in structure as set forth in the Provision titled Compliance Reporting. Delivery must occur within seven (7) days of entry of this Order for current personnel. For all others, delivery must occur within seven (7) days of assuming their responsibilities.

C. From each individual or entity to which a Defendant delivered a copy of this Order, that Defendant must obtain, within thirty (30) days, a signed and dated acknowledgment of receipt of this Order.

XVII. COMPLIANCE REPORTING

IT IS FURTHER ORDERED that Defendants make timely submissions to the Commission and the Division:

A. One year after entry of this Order, Defendants must submit a compliance report, sworn under penalty of perjury:

1. Each Defendant must: (a) identify the primary physical, postal, and email address and telephone number, as designated points of contact, which representatives of the Commission and the Division, may use to communicate with Defendant; (b) identify all of that Defendant's businesses by all of their names, telephone numbers, and physical, postal, email, and Internet addresses; (c) describe the activities of each business, including the goods and services offered, the means of advertising, marketing, and sales, and the involvement of any other Defendant; (d) describe in detail whether and how that Defendant is in compliance with each Provision of this Order; and (e) provide a copy of each Order Acknowledgment obtained pursuant to this Order, unless previously submitted to the Commission and the Division.

B. For ten (10) years after entry of this Order, Defendants must submit a compliance notice, sworn under penalty of perjury, within fourteen (14) days of any change in the following:

1. Each Defendant must report any change in: (a) any designated point of contact; or (b) the structure of any Defendant or any entity that Defendant has any ownership interest in or controls directly or indirectly that may affect compliance obligations arising under this Order, including: creation, merger, sale, or dissolution of the entity or any subsidiary, parent, or affiliate that engages in any acts or practices subject to this Order.

C. Defendants must submit to the Commission and the Division notice of the filing of any bankruptcy petition, insolvency proceeding, or similar proceeding by or against any such Defendant within fourteen (14) days of its filing.

D. Any submission to the Commission and the Division required by this Order to be sworn under penalty of perjury must be true and accurate and comply with 28 U.S.C. § 1746, such as by concluding: "I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on: _____" and supplying the date, signatory's full name, title (if applicable), and signature.

E. Unless otherwise directed by a Commission representative in writing, all submissions to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580, and via email to WCCE@agutah.gov or by overnight courier (not the U.S. Postal Service) to the Utah Attorney General's Office, White Collar and Commercial Enforcement Division, 160 East 300 South, 5th Floor, Salt Lake City, UT 84114. The subject line must begin: "FTC v. MindGeek, FTC File No. 2123033."

XVIII. RECORDKEEPING

IT IS FURTHER ORDERED that Defendants must create certain records for ten (10) years after entry of this Order, and retain each such record for five (5) years. Specifically, Defendants must create and retain the following records:

A. Accounting records showing the revenues from all goods or services sold, the costs incurred in generating those revenues, and resulting net profit or loss;

B. Personnel records showing, for each person providing services in relation to any aspect of the Order, whether as an employee or otherwise, that person's: name; addresses; telephone numbers; job title or position; dates of service; and (if applicable) the reason for termination;

C. Records of all consumer complaints and refund requests, whether received directly or indirectly, such as through a third party, and any response;

D. All records necessary to demonstrate full compliance with each provision of this Order, including all submissions to the Commission and the Division;

E. A copy of each unique advertisement or other marketing material making a representation subject to this Order;

F. A copy of each widely disseminated representation by Defendants that describes the extent to which Defendants maintain or protect the privacy, security and confidentiality of any Covered Information, including any representation concerning a change in any website or other service controlled by Defendants that relates to the privacy, security, and confidentiality of Covered Information;

G. For five (5) years after the date of preparation of each Assessment required by this Order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of Defendants, including all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials concerning Defendants' compliance with related Provisions of this Order, for the compliance period covered by such Assessment; and

H. For five (5) years from the date received, copies of all subpoenas and other communications with law enforcement, if such communications relate to Defendants' compliance with this Order.

XIX. COMPLIANCE MONITORING

IT IS FURTHER ORDERED that, for the purpose of monitoring Defendants' compliance with this Order:

A. Within fourteen (14) days of receipt of a written request from a representative of the Commission or the Division, each Defendant must: submit additional compliance reports or other requested information, which must be sworn under penalty of perjury; appear for depositions; and produce documents for inspection and copying. The Commission and the Division are also authorized to obtain discovery, without further leave of court, using any of the procedures prescribed by Federal Rules of Civil Procedure 29, 30 (including depositions by remote means), 31, 33, 34, 36, 45, and 69.

B. For matters concerning this Order, the Commission and the Division are each authorized to communicate directly with each Defendant. Defendants must permit representatives of the Commission or the Division to interview any employee or other person affiliated with any Defendant who has agreed to such an interview. The person interviewed may have counsel present.

C. The Commission or the Division may use all other lawful means, including posing through its representatives as consumers, suppliers, or other individuals or entities, to Defendants or any individual or entity affiliated with Defendants, without the necessity of identification or prior notice. Nothing in this Order limits the Commission's lawful use of compulsory process, pursuant to Sections 9 and 20 of the FTC Act, 15 U.S.C. §§ 49, 57b-1. Nothing in this Order limits the Division's lawful use of compulsory process pursuant to Utah Code sections 13-2-5, 6, and 13-11-8, 16, 17.

D. Defendants will not take any action, enter into any agreement, or assist any other party to transfer the management or operation of www.pornhub.com or any other Covered Service in any manner that is intended to evade, or could reasonably be expected to evade, any requirements set forth in this Order.

XX. RETENTION OF JURISDICTION

IT IS FURTHER ORDERED that this Court retains jurisdiction of this matter for purposes of construction, modification, and enforcement of this Order.

SO ORDERED this 8th day of September, 2025.

Ted Stewart
UNITED STATES DISTRICT JUDGE

SO STIPULATED AND AGREED:

FOR PLAINTIFFS:

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

Docusign Envelope ID: 2A3BEFE2-9532-4DCF-A787-5A895EA055DE

FOR DEFENDANTS:

Dated: 7/9/2025

Gregory P. Luib
Dechert LLP
1900 K Street, **N.W.**
Washington, D.C. 20006
Telephone: (202) 261-3413
gregory.luib@dechert.com

Ryan T. Andrews
Quinn Emanuel Urquhart & Sullivan, LLP
1300 I Street, **N.W.,** Suite 900
Washington, D.C. 20005
Telephone: (202) 538-8155
ryanandrews@quinnemanuel.com

Attorneys for Defendants

FOR DEFENDANT AYLO GROUP LTD.:

Dated: 7/8/2025

Signed by:
andreas alkiviades andreou
BC960CBBEAF248...
Andreas Alkiviades Andreou
Director

FOR DEFENDANT DONORMASS LIMITED:

Dated: 7/8/2025

Signed by:
andreas alkiviades andreou
BC969CBBEAF2454...

Andreas Alkiviades Andreou
Director

FOR DEFENDANT AYLO FREESITES LTD.:

Dated: 7/8/2025

Signed by:
andreas alkiviades andreou
BC969CBBEAF2454...

Andreas Alkiviades Andreou
Director

FOR DEFENDANT AYLO PREMIUM LTD.:

Dated: 7/8/2025

Signed by:
andreas alkiviades andreou
BC969CBBEAF2454...

Andreas Alkiviades Andreou
Director

FOR DEFENDANT AYLO TECHNOLOGIES LTD.:

Dated: 7/8/2025

Signed by:
andreas alkiviades andreou
BC969CBBEAF2454...

Andreas Alkiviades Andreou
Director

FOR DEFENDANT 9279-2738 QUEBEC INC.:

Dated: 7/8/2025

Signed by:
andreas alkiviades andreou
BC969CBBEAF2454...

Andreas Alkiviades Andreou
Director

FOR DEFENDANT 9219-1568 QUEBEC INC.:

Dated: 7/8/2025

Signed by:
andreas alkiviades andreou
BC969CBBEAF2454...

Andreas Alkiviades Andreou
Director

FOR DEFENDANT AYLO HOLDINGS USA CORP.:

Dated: 7/9/2025

Signed by:
Andrew Link
F542F7F10EE744D...

Andrew Link
Director

FOR DEFENDANT AYLO BILLING US CORP.:

Dated: 7/9/2025

Signed by:
Andrew Link
F542F7F10EE744D...

Andrew Link
Director

FOR DEFENDANT TOQON, LLC:

Dated: 7/9/2025

Signed by:
Andrew Link
F542F7F10EE744D...

Andrew Link
Manager

FOR DEFENDANT AYLO GLOBAL ENTERTAINMENT INC.:

Dated: 7/9/2025

Signed by:
Andrew Link
F542F7F10EE744D...

Andrew Link
Director

FOR DEFENDANT AYLO USA INCORPORATED:

Dated: 7/9/2025

Signed by:
Andrew Link
F542F7F10EE744D...

Andrew Link
Director

FOR DEFENDANT FTSA, LLC:

Dated: 7/9/2025

Signed by:
Anis Baba
B8CAFF8007C2448...

Anis Baba
Manager

FOR DEFENDANT AYLO BILLING LIMITED:

Dated: 7/8/2025

Signed by:
andreas alkiviades andreou
BC969CBBEAF2454...

Andreas Alkiviades Andreou
Director

EXHIBIT A

Exhibit A

Website and Mobile Application Notice

[To appear with the Aylo logo]

The Steps We're Taking to Stop the Publication of Child Sexual Abuse Material and Non-Consensual Material

CONTENT WARNING: This message contains references to sensitive content, including sexually explicit content involving minors and non-consensual acts.

Aylo owns and operates several free, ad-based websites, including Pornhub.com, Youporn.com, Redtube.com, Tube8.com, and Thumbzilla.com, as well as subscription-based websites associated with its free sites, including Pornhubpremium.com ("Websites").

The Federal Trade Commission ("FTC") and the Utah Division of Consumer Protection ("Utah") allege that some of our Websites made available videos and photos containing child sexual abuse material ("CSAM") as well as non-consensual material ("NCM"), such as revenge porn and spy camera videos.

We've entered into an agreement with the FTC and Utah that requires us to take steps to keep CSAM and NCM off of our Websites. To resolve the case, we must have a comprehensive program with robust safeguards to:

- Verify that uploaders of pornographic content to our Websites are at least 18 years old;
- Verify that performers in pornographic content on our Websites are at least 18 years old;
- Verify that performers in pornographic content on our Websites have given written consent to the production and publication of the pornographic content;
- Allow performers to request to have content they appear in removed from our Websites [hyperlink to where can submit withdrawal of consent request]
- Allow registered users to report CSAM and/or NCM on our Websites by flagging content, comments, and direct messages;
- Allow users to request removal of CSAM and/or NCM from our Websites [hyperlink to where can submit content removal requests];
- Remove actual or suspected CSAM and/or NCM Aylo becomes aware of from all of our Websites; and
- Publish a report twice a year describing how we are taking steps to prevent CSAM and/or NCM from appearing on our platforms.

An independent third party will audit our practices to make sure we are taking steps to prevent CSAM and NCM from appearing on our Websites. These audits will happen every two years for the next 10 years.

Learn more.

If you have any questions, email us at [email address].

To learn more about the settlement, go to ftc.gov and search for "Aylo."

If you have any concerns about our practices, you can report them to the FTC at ReportFraud.ftc.gov.