2123091
UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Lina M. Khan, Chair**
Rebecca Kelly Slaughter
Alvaro M. Bedoya

In the Matter of **FACEBOOK, Inc.,** ***a corporation.***	**Docket No. C-4365**

PROPOSED DECISION AND ORDER

The Federal Trade Commission ("Commission") initiated an investigation of certain acts and practices of the Respondent named in the caption. Following that investigation, the Commission, pursuant to 15 U.S.C. § 45(b) and 16 C.F.R. § 3.72(b), issued its Order to Show Cause why the Commission should not modify its Decision and Order, *In the Matter of Facebook, Inc.*, Docket No. C-4365 (July 27, 2012), *as modified by* Order Modifying Prior Decision and Order, *In the Matter of Facebook, Inc.*, Docket No. C-4365 (Apr. 27, 2020).

The Commission, having provided Respondent notice and opportunity for hearing, hereby issues the following Order:

FINDINGS

Respondent

1. Respondent Facebook, Inc. is a Delaware corporation with its principal office or place of business at 1601 Willow Road, Menlo Park, California 94025.

2. On October 29, 2021, Respondent notified the Commission that Facebook, Inc. changed its name to Meta Platforms, Inc., and reported that Meta Platforms, Inc. would replace Facebook, Inc. as Respondent in the Commission's orders.

Prior Commission Actions

3. In 2012, the Commission sued Respondent for promising users they could restrict the sharing of their non-public personal information to limited audiences, when in fact such limitations did not prevent Respondent from sharing the users' information with third-party

developers. Respondent entered into a consent order to settle that matter. *See* Decision and Order, *In the Matter of Facebook, Inc.*, Docket No. C-4365 (July 27, 2012) ("2012 Order").

4. In 2019, following the Commission's investigation, and acting upon notification and authorization by the Commission, the United States Department of Justice ("DOJ") filed a complaint ("2019 Case") in the United States District Court for the District of Columbia charging Respondent with multiple violations of the 2012 Order and Section 5(a) of the FTC Act, 15 U.S.C. § 45(a) ("Section 5"). This 2019 Case alleged Respondent violated the 2012 Order in three ways: (1) misrepresenting the extent to which users could control the privacy of their data and the steps they needed to take to implement such controls; (2) misrepresenting the information the Company made accessible to third parties; and (3) failing to establish, implement, and maintain a privacy program reasonably designed to address privacy risks. The 2019 Case also alleged Respondent violated Section 5 when it told users it would collect their telephone numbers to enable a security feature but did not disclose it also used those numbers for advertising.

5. To resolve the 2019 Case, on or about July 23, 2019, Respondent agreed to the entry of a Stipulated Order for Civil Penalty, Monetary Judgment, and Injunctive Relief. As part of this agreement, Respondent consented to reopening the administrative proceedings at docket number C-4365 to modify the 2012 Order with a revised Decision and Order. *See* Order Modifying Prior Decision and Order, *In the Matter of Facebook, Inc.*, Docket No. C-4365 (Apr. 27, 2020) ("2020 Order").

Respondent's Privacy Program

6. The 2020 Order requires Respondent to establish, implement, and maintain a comprehensive privacy program that "protects the privacy, confidentiality, and integrity of the Covered Information collected, used, or shared" by Respondent. The 2020 Order specifies the minimum requirements for the program and requires Respondent to obtain initial and biennial assessments of its privacy program from an independent third-party professional.

7. Pursuant to the 2020 Order, Respondent selected and, together with DOJ, Commission staff approved Protiviti, Inc. as Respondent's Independent Assessor ("Assessor").

8. On July 1, 2021, pursuant to Part VIII of the 2020 Order, Respondent submitted its Assessor's initial report for October 25, 2020 to April 22, 2021.

9. Through its testing and analysis, the Assessor identified [redacted] individual gaps and weaknesses of varying significance [redacted] into which Respondent's privacy program is organized.

10. The Assessor found that although "the key foundational elements necessary for an effective program are now in place, . . . their maturity and completeness vary from [redacted]." Thus, the Assessor concluded "the gaps and weaknesses noted within our review demonstrate that substantial additional work is required, and additional investments must be made, in order for the program to mature [redacted]."

Respondent's Misrepresentations

11. From 2018 through June 2020, Respondent misrepresented the extent to which third-party developers could receive non-public information.

12. Specifically, on or about April 11, 2018, Respondent announced it would remove app developers' access to a user's data if that user had not used the app in the prior 90 days (the "90-Day Limitation"). Respondent represented these "Expired Apps" would be permitted to retain data they had obtained while the user was still active but would be unable to continue obtaining the user's nonpublic information.

13. Respondent conveyed the change to users through representations in several places: the Apps and Websites setting; the Help Center; and the Data Policy.

14. For some users, Respondent's representations were false. Respondent had in fact, in some instances, continued to share users' nonpublic information with Expired Apps. Moreover, this sharing had been occurring since Respondent launched the feature in April 2018.

15. Respondent's misrepresentations regarding its 90-Day Limitation feature violated Section 5 of the FTC Act, Part I of the 2012 Order for the period prior to the issuance of the 2020 Order, and Part I of the 2020 Order thereafter.

16. From December 2017 to July 2019, Respondent also made misrepresentations relating to its Messenger Kids ("MK") product, a free messaging and video calling application "specifically intended for users under the age of 13."

17. Beginning when the app started in December 2017 and throughout its operation, Respondent represented that MK users could communicate in MK with only parent-approved contacts. However, Respondent made coding errors that resulted in children participating in group text chats and group video calls with unapproved contacts under certain circumstances.

18. Specifically, from June 2018 to July 2, 2019, when MK users initiated a group text chat on Android devices by simultaneously selecting multiple contacts to participate in the chat, coding errors caused the application to fail to check whether the secondary contacts were approved to chat with each other. This resulted in certain MK users communicating with unapproved contacts in group text chats.

19. Separately, some MK users participated in group video calls with unapproved contacts due to a different coding error. Specifically, in November 2018, a coding error allowed Messenger users to add other individuals to ongoing video calls with MK users through a feature called escalation. Technical safeguards implemented to prevent MK users from communicating with unapproved contacts failed to work with the escalation feature, thereby resulting in MK users communicating with unapproved contacts through group video calls. Respondent fixed this coding error in January 2019. Similarly, in May 2019, another error again allowed certain Messenger users to add individuals to ongoing video calls with MK users. Respondent fixed the second group video call error on or about July 2, 2019.

20. Respondent's misrepresentations regarding Messenger Kids violated Part I of the 2012

Order, Section 5 of the FTC Act, the Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. § 6502, and the Children's Online Privacy Protection Rule ("COPPA Rule"), 16 C.F.R. Part 312.

DEFINITIONS

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

A. "**Affected Facial Recognition User**" means any User who has a "Tag Suggestions" setting as of the effective date of this Order, any User who signs up for Respondent's service after the effective date of this Order and has received the "Tag Suggestions" setting, and any User whose biometric information has been collected by Respondent for any other purpose.

B. "**Affirmative Express Consent**" means any freely given, specific, informed, and unambiguous indication of an individual User's wishes demonstrating agreement by the individual, such as by a clear affirmative action, following a Clear and Conspicuous disclosure to the individual of: (1) the categories of information that will be collected; (2) the specific purpose(s) for which such data will be collected, used, or disclosed; (3) the name(s) of any entity that collects the information or to which the information is disclosed; (4) a simple, easily located means for the User to withdraw consent; (5) any limitations on the User's ability to withdraw consent; and (6) all other information material to the provision of consent. The Clear and Conspicuous disclosure must be separate from any "privacy policy," "terms of service," "terms of use," or other similar document.

The following does not constitute Affirmative Express Consent:

a Inferring consent from the hovering over, muting, pausing, or closing of a given piece of content by the consumer; or

b. Obtaining consent through a User interface that has the substantial effect of subverting or impairing User autonomy, decision-making, or choice.

C. "**Algorithm**" means a process of examining and analyzing data in order to find patterns and make conclusions about that data, whether by machine or human analysis.

D. "**Acquisition**" means the purchase of one company by another to fulfill particular strategic goals, such as those related to revenues, market share, product or service offerings, or competition. An Acquisition may be structured as an acquisition of stock, assets (including, but not limited to, the acquisition of applications or websites, contracts, patents, intellectual property, or data), talent (e.g., employees or staff), or any combination thereof.

E. "**Child**" or "**Children**" means individual(s) under the age of thirteen (13).

F. "**Clear(ly) and Conspicuous(ly)**" means that a required disclosure is difficult to miss (i.e., easily noticeable) 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 video or 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 is made in 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 representation that requires the disclosure 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 reasonable members of that group.

G. "**Commitment**" means any representation to consumers, whether located in a privacy or data policy, terms of use, setting, consent flow, User interface or notice, press release, blog post or otherwise, relating to the collection, storage, maintenance, use, sharing, provision of access to, selling, or deletion of Covered Information.

H. "**Covered Incident**" means any instance in which Respondent has verified or otherwise confirmed that the Covered Information of 500 or more consumers was or was likely to have been accessed, collected, used, maintained, or shared in a manner that violates Respondent's Commitments or Platform Terms.

I. "**Covered Information**" means information from or about an individual consumer including, but not limited to: (1) a first or last name; (2) geolocation information sufficient

to identify a 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 mobile or other telephone number; (5) photos and videos; (6 Internet Protocol ("IP") address, User ID, or other persistent identifier that can be used to recognize a User over time and across different devices, websites or online services; (7) a Social Security number; (8) a driver's license or other government-issued identification number; (9) financial account number; (10) credit or debit information; (11) date of birth; (12) biometric information; (13) any information combined with any of (1) through (12) above; or (n) Nonpublic User Information.

J. "**Covered Third Party**" means any individual or entity that uses or receives Covered Information obtained by or on behalf of Respondent outside of a User-initiated transfer of Covered Information as part of a data portability protocol or standard, other than: (1) a service provider of Respondent that (i) uses the Covered Information for and at the direction of Respondent and no other individual or entity and for no other purpose; and (ii) does not disclose the Covered Information, or any individually identifiable information derived from such Covered Information, except for, and at the direction of, Respondent, for the purpose of providing services requested by a User and for no other purpose; or (2) any entity that uses the Covered Information only as reasonably necessary: (i) to comply with applicable law, regulation, or legal process; or (ii) to enforce Respondent's terms of use; or (iii) to detect, prevent, or mitigate fraud or security vulnerabilities.

K. "**Facial Recognition Template**" means data, such as a unique combination of numbers or other alphanumeric characters, that is used to predict if the face of a specific User is represented in an image or other visual content.

L. "**Independent Director**" means a member of Respondent's Board of Directors other than an executive officer or employee of Respondent or any other individual having a relationship that, in the opinion of the Independent Nominating Committee, would interfere with the exercise of independent judgment in carrying out the responsibilities of such director.

M. "**Independent Privacy Committee**" means a committee of Respondent's Board of Directors, consisting of Independent Directors, all of whom meet the Privacy and Compliance Baseline Requirements. At least one Independent Director on the Independent Privacy Committee must hold a position, or have held such a position within the last five (5) years, at a nonprofit where that person has worked, in whole or in part, to safeguard civil liberties, protect consumers from data abuses, strengthen consumer privacy standards online, research or advocate for consumer privacy protections, or enforce consumer privacy laws.

N. "**Independent Nominating Committee**" means a committee of Respondent's Board of Directors, consisting of Independent Directors, the charter of which will encompass, among other things, approving for nomination individuals to the Respondent's Board of Directors and to the Independent Privacy Committee.

O. "**Integrity**" means the protection of information from unauthorized destruction, corruption, or falsification.

P. "**Nonpublic User Information**" means any User profile information (i.e., information that a User adds to or is listed on a User's Facebook profile), or other User information (e.g., status updates, photos) that is restricted by one or more Privacy Setting(s) or is otherwise not publicly available on a User's profile, timeline, or newsfeed.

Q. "**Platform Terms**" means Respondent's written terms, policies, and procedures relating to the privacy, confidentiality, security, or Integrity of Covered Information that apply to Covered Third Parties.

R. "**Principal Executive Officer**" means Mark Zuckerberg for so long as he serves as Chief Executive Officer or President of Respondent, or such other officer (regardless of title) that is designated in Respondent's bylaws or by resolution of the Board of Directors as having the duties of the Principal Executive Officer of Respondent, acting solely in his official capacity on behalf of Respondent; or if Mark Zuckerberg no longer serves in such a position, then such other individual serving as the Chief Executive Officer of Respondent, or such other officer (regardless of title) that is designated in Respondent's bylaws or by resolution of the Board of Directors as having the duties of the Principal Executive Officer of Respondent, acting solely in his or her official capacity on behalf of Respondent. In the event that Mark Zuckerberg is not the Principal Executive Officer and such position is jointly held by two or more persons, then each of such persons shall be deemed to be a Principal Executive Officer.

S. "**Privacy and Compliance Baseline Requirements**" refers to the requirements that, in the opinion of the Independent Nominating Committee, a member of the Independent Privacy Committee has (1) the ability to understand corporate compliance and accountability programs and to read and understand data protection and privacy policies and procedures; and (2) such other relevant privacy and compliance experience reasonably necessary to exercise his or her duties on the Independent Privacy Committee.

T. "**Privacy Risks and Harms**" refers to the risk to the privacy, confidentiality, security, or Integrity of Covered Information that could result in the unauthorized access to, collection, use, retention, or destruction of such information; and the risk of harm caused, directly or indirectly, by the access to, or collection, use, retention, or destruction, of Covered Information, including physical harm, emotional distress or mental health harm, economic harm, reputational harm, relationship harm, discrimination, or harm to an individual's autonomy (e.g., impairing an individual's ability to make his or her own informed decisions, such as through coercion, manipulation, thwarted expectations, or failure to inform the individual of material facts).

U. "**Privacy Setting**" includes any control or setting provided by Respondent that allows a User to decide how the User's Covered Information is accessed, collected, used, retained, or destroyed.

V. "**Representatives**" means Respondent's officers, agents, servants, employees, attorneys, and those persons in active concert or participation with them who receive actual notice of this Order by personal service or otherwise.

W. "**Respondent**" means Meta Platforms, Inc., (f/k/a Facebook, Inc. and Facebook), its successors and assigns, acting directly, or through any corporation, company, subsidiary, division, affiliate, website, or other device that it directly or indirectly controls.

X. "**Teen**" or "**Teens**" means an individual between the ages of thirteen (13) and seventeen (17), inclusively.

Y. "**User**" means an identified individual from whom Respondent has obtained information for the purpose of providing access to Respondent's products and services.

Z. "**Youth**" means Children and Teens.

PROVISIONS

I. PROHIBITION ON THE HANDLING OF COVERED INFORMATION FROM YOUTH USERS

IT IS ORDERED that Respondent and its Representatives, whether acting directly or indirectly, in connection with any commercial website or online service, or portion thereof, for which it is collecting, using, or maintaining Covered Information from or about Youth Users, are hereby permanently restrained and enjoined from:

A. Collecting, using, selling, licensing, transferring, sharing, disclosing, or otherwise benefitting from Covered Information from Youth Users, except for the purposes of operating the website or online service; maintaining or analyzing the functioning of the website or online service; performing network communications; authenticating Youth Users and their Covered Information; protecting the privacy, confidentiality, security, or Integrity of the website, online service, or its Youth Users; or ensuring legal or regulatory compliance. This prohibition includes collecting, using, selling, licensing, transferring, sharing, disclosing, or otherwise benefitting from Covered Information collected from Youth Users for the purposes of developing, training, refining, improving, or otherwise benefiting Algorithms or models; serving targeted advertising; or enriching Respondent's data on Youth Users. Furthermore, Respondent shall not condition the availability of any product, feature, or service on the collection of a User's facial recognition or other biometric data unless it is necessary to enable that specific product, feature, or service, and the information is used solely for that purpose;

B. Failing to develop and implement policies and practices that: (1) permit each User to delete Covered Information collected prior to the User's eighteenth birthday; (2) require Respondent to delete Covered Information collected from a User as a Youth unless Respondent obtains Affirmative Express Consent from the User within a reasonable time period, not to exceed six (6) months after the User's eighteenth birthday; and (3) require Respondent to post a prominent and clearly labeled link to an online notice that states how Users can request deletion of

Covered Information collected prior to their eighteenth birthday; and

C. Failing to update its terms of service and privacy policy to reflect the requirements set forth in the above subparts I.A. and I.B. .

II. PROHIBITION AGAINST MISREPRESENTATIONS

IT IS FURTHER ORDERED that Respondent, including Representatives of Respondent, in connection with any product or service, shall not misrepresent in any manner, expressly or by implication, the extent to which Respondent maintains the privacy, confidentiality, security, or Integrity of Covered Information, including, but not limited to:

A. Its collection, use, access to, or disclosure of any Covered Information;

B. The extent to which a consumer can control the privacy of any Covered Information maintained by Respondent and the steps a consumer must take to implement such controls;

C. The extent to which Respondent makes or has made Covered Information accessible to third parties;

D. The steps Respondent takes or has taken to verify the privacy or security protections that any third party provides;

E. The extent to which Respondent makes or has made Covered Information accessible to any third party following deletion or termination of a User's account with Respondent or during such time as a User's account is deactivated or suspended; and

F. The extent to which Respondent is a member of, adheres to, complies with, is certified by, is endorsed by, or otherwise participates in any privacy or security program sponsored by a government or any self-regulatory or standard-setting organization, including but not limited to the EU-U.S. Privacy Shield framework, the Swiss-U.S. Privacy Shield framework, and the APEC Cross-Border Privacy Rules.

III. CHANGES TO SHARING OF NONPUBLIC USER INFORMATION

IT IS FURTHER ORDERED that Respondent and its Representatives, in connection with any product or service in or affecting commerce, prior to any access to, collection, use, or of a User's Nonpublic User Information by Respondent with any Covered Third Party which exceeds the restrictions imposed by a User's Privacy Setting(s), shall:

A. Clearly and Conspicuously disclose (such as in a stand-alone disclosure or notice) to the User, separate and apart from any "privacy policy," "data use policy," "statement of rights and responsibilities" page, or other similar document: (1) the categories of Nonpublic User Information that will be collected, used, or disclosed to such Covered Third Parties; (2) the identity or specific categories of such Covered Third Parties; and (3) that such access to, collection, or use exceeds the restrictions imposed by the Privacy Setting(s) in effect for the User;

and

B. Obtain the User's Affirmative Express Consent.

Nothing in Part III will: (1) limit the applicability of Part II of this Order; or (2) require Respondent to obtain Affirmative Express Consent for sharing of a User's Nonpublic User Information initiated by another User authorized to access such information, provided that such sharing does not materially exceed the restrictions imposed by a User's Privacy Setting(s). Respondent may seek modification of this Part pursuant to 15 U.S.C. § 45(b) and 16 C.F.R. § 2.51(b) to address relevant developments that affect compliance with this Part, including, but not limited to, technological changes and changes in methods of obtaining Affirmative Express Consent.

IV. DELETION OF INFORMATION

IT IS FURTHER ORDERED that Respondent and its Representatives, in connection with any product or service, must create, within ninety (90) days of the effective date of this Order, a comprehensive data map that documents, for each element of Covered Information stored in each data map: (i) the type of Covered Information (e.g. Mobile Advertising ID); (ii) the source(s) of collection; (iii) the particular purpose(s) for which Covered Information was collected; (iv) each use of that type of Covered Information; (v) the retention schedule; and (vi) the location of each data store that contains each type of Covered Information.. Any new database containing Covered Information must be added to the comprehensive data map within twenty (20) days of its creation. This data map must be maintained and kept up to date.

Within a reasonable period, not to exceed thirty (30) days, after a User deletes his or her data or deletes or terminates his or her account, Respondent must ensure that Covered Information regarding that User cannot be accessed by any Covered Third Party, except as required by law or where necessary to protect Respondent's website or its Users from fraud or illegal activity.

Additionally, Respondent and its Representatives must ensure that Covered Information entered by the User (such as User-generated content) is deleted from servers under Respondent's control, or is de-identified such that it is no longer associated with the User and the User's account or device, within a reasonable period (not to exceed 120 days) from the time that the User has deleted such information, or his or her account, except: (1) as required by law; (2) where necessary for the safety and security of Respondent's products, services, features, and Users, including to prevent fraud or other malicious activity; (3) where stored solely for backup or disaster recovery purposes (subject to a retention period necessary to provide a reliable service); or (4) where technically infeasible given Respondent's existing systems.

V. LIMITATIONS ON THE USE OR SHARING OF TELEPHONE NUMBERS SPECIFICALLY PROVIDED TO ENABLE ACCOUNT SECURITY FEATURES

IT IS FURTHER ORDERED that Respondent and its Representatives, in connection with any product or service, shall not use for the purpose of serving advertisements, or share with any Covered Third Party for such purpose, any telephone number obtained from a User prior to the effective date of this Order for the specific purpose of enabling an account security feature designed to protect against unauthorized account access (i.e., two-factor authentication, password recovery, and login alerts). Nothing in Part V will limit Respondent's ability to use such telephone numbers if obtained separate and apart from a User enabling such account security feature and in a manner consistent with the requirements of this Order.

VI. COVERED INFORMATION AND USER PASSWORD SECURITY

IT IS FURTHER ORDERED that Respondent and its Representatives, in connection with any product or service, must implement, and thereafter maintain, a comprehensive information security program designed to protect the security of Covered Information. In addition to any security-related measures associated with Respondent's Mandated Privacy Program under Part VIII of this Order, the information security program must contain safeguards appropriate to Respondent's size and complexity, the nature and scope of Respondent's activities, and the sensitivity of the Covered Information. Specifically with respect to the collection, storage, transit, or use of User passwords, such safeguards shall include:

A. Not requesting or requiring, as part of the User log-in, authentication, or account creation process, User passwords to independent, third-party consumer applications, websites, or other services;

B. Cryptographically protecting or otherwise securing User passwords when stored and when in transit over the Internet or other similar transmission channel; and

C. Implementing regular automated scans designed to detect whether Respondent is storing any User passwords in plaintext, and cryptographically protecting, deleting, or otherwise rendering unreadable any such passwords.

VII. FACIAL RECOGNITION TEMPLATES

IT IS FURTHER ORDERED that Respondent and its Representatives, in connection with any product or service, in or affecting commerce, shall not create any new Facial Recognition Templates for any Affected Facial Recognition User, unless Respondent Clearly and Conspicuously discloses (such as in a stand-alone disclosure or notice), separate and apart from any "privacy policy," "data policy," "statement of rights and responsibilities" page, or other similar documents, how Respondent will use, and to the extent applicable, share, the Facial Recognition Templates for such User, and obtains such User's Affirmative Express Consent.

VIII. MANDATED PRIVACY PROGRAM

IT IS FURTHER ORDERED that Respondent, in connection with any product, service, or sharing of Covered Information, shall establish and implement, and thereafter maintain a comprehensive privacy program ("Mandated Privacy Program") that effectively mitigates Privacy Risks and Harms. To satisfy this requirement, Respondent must, within 180 days of the effective date of this Order, at a minimum:

A. Document in writing the content, implementation, and maintenance of the Mandated Privacy Program that includes: (1) the documented risk assessment required under subpart VIII.D. of this Order; (2) the documented safeguards required under subpart VIII.E. of this Order, including the implementation status of such safeguards and any known safeguards or other alternative procedures that would mitigate the identified Privacy Risks and Harms, but which were not implemented and each reason such procedure(s) were not implemented; (3) the identification of any residual Privacy Risks and Harms that were not mitigated by the documented safeguards identified in subpart VIII.A(2); (4) a description of the training required under subpart VIII.H. of this Order; (5) a description of the procedures adopted for handling Covered Information for Youth Users required under Part I of this Order; and (6) a description of the procedures adopted for implementing and monitoring the Mandated Privacy Program, including procedures used for evaluating and adjusting the Mandated Privacy Program as required under subpart VIII.K. of this Order;

B. Provide the written program required under subpart VIII.A. of this Order, and any evaluations thereof or adjustments thereto, to the Principal Executive Officer and to the Independent Privacy Committee created in response to Part XII of this Order at least once every twelve (12) months;

C. Designate a qualified employee or employees to coordinate and be responsible for the Mandated Privacy Program ("Designated Compliance Officer(s)"), one of whom will be the Chief Privacy Officer for Product, subject to the reasonable approval of the Independent Privacy Committee, and who may only be removed from such position by Respondent with an affirmative vote of a majority of the Independent Privacy Committee;

D. Conduct and document, at least once every twelve (12) months, a comprehensive risk assessment of the internal and external Privacy Risks and Harms in each area of its operation (e.g., employee training and management; developer operations; partnerships with Covered Third Parties; sharing of Covered Information with Covered Third Parties or Facebook-owned affiliates; product research, design, and development; advertising; and product marketing and implementation). This assessment must include an evaluation of: (1) each individual product or service feature that collects, uses or shares Covered Information, both on a standalone basis and within the context of the broader product or service that the feature will be supporting or operating (e.g., considering the product or service inclusive of all relevant features); (2) whether existing and fully implemented safeguards effectively mitigate the identified Privacy Risks and Harms for each product or service; (3) whether additional safeguards are available that could better mitigate the identified Privacy Risks and Harms or address any residual unresolved Privacy Risks and Harms; (4) the sufficiency of any proposed User notice and, if necessary, consent; and (5) whether

the product or service feature should be deprecated or removed. Respondent shall further assess and document the internal and external Privacy Risks and Harms described above as they relate to a Covered Incident promptly following verification or confirmation of such an incident, in any event not to exceed thirty (30) days after the Covered Incident is verified or otherwise confirmed;

E. Design, implement, maintain, and document safeguards that control for the material internal and external Privacy Risks and Harms identified by Respondent in response to subpart VIII.D. Each safeguard shall be based on the volume and sensitivity of the Covered Information that is at risk, the severity of the potential Privacy Risks and Harms; and the likelihood that the Privacy Risks and Harms could be realized;

1. Specifically with respect to any Covered Third Party that obtains or otherwise has access to Covered Information from Respondent for use in an independent, third-party consumer application or website, such safeguards shall include:

a. Requiring an annual self-certification by each Covered Third Party that certifies: (i) its compliance with each of Respondent's Platform Terms; and (ii) the purpose(s) or use(s) for each type of Covered Information to which it requests or continues to have access, and that each specified purpose or use complies with Respondent's Platform Terms;

b. Denying or terminating access to any type of Covered Information that the Covered Third Party fails to certify pursuant to subpart VIII.E.1.a.(ii) above, or, if the Covered Third Party fails to complete the annual self-certification, denying or terminating access to all Covered Information unless the Covered Third Party cures such failure within a reasonable time, not to exceed thirty (30) days;

c. Monitoring Covered Third Party compliance with Respondent's Platform Terms through measures including, but not limited to, ongoing manual reviews and automated scans, and regular assessments, audits, or other technical and operational testing at least once every twelve (12) months;

d. Conducting, at least once every twelve (12) months, enhanced monitoring of higher risk Covered Third Parties, which are Covered Third Parties that obtain permissions to Covered Information beyond a user's name, User ID, Username, Profile Picture/Avatar, and account type. Beyond the pre-existing safeguards for all Covered Third Parties set forth in subparts VIII.E.1.a. through c. above, Respondent must, for higher-risk Covered Third Parties: (i) require more comprehensive assessments of the Platform Terms compliance by Covered Third Parties (e.g., more detailed questionnaires, evidence certifying the results of vulnerability assessments); (ii) review responses to the assessments, flag any practices inconsistent with Respondent's Platform Terms, and address them directly with the appropriate Covered Third Party; and (iii) conduct higher sampling ratios of assessments and hands-on audits driven by the level of risk assessment for the Covered Third Parties, including an individual review of a sample of higher risk Covered Third Party applications; and

e. Timely enforcing against any Covered Third Party violations of Respondent's Platform Terms based solely on the severity, nature, and impact of the violation, the Covered Third Party's malicious conduct or history of violations, and applicable law.

2. Specifically with respect to Respondent's collection, use, or sharing of Covered Information in any new or modified product, service, or practice, such safeguards shall include:

a. Prior to implementing any new or modified product, service, or practice, including any relevant individual feature(s) thereof:

(i) Conducting and documenting a comprehensive risk assessment of the internal and external Privacy Risks and Harms associated with the new or modified product, service, or practice ("Privacy Review"). This assessment must include an evaluation of: (a) the new or modified individual product or service feature that collects, uses, or shares Covered Information, both on a standalone basis and within the context of the broader product or service that the feature will be supporting or operating (e.g., considering the product or service inclusive of all relevant features); (b) whether existing and fully implemented safeguards effectively mitigate the identified Privacy Risks and Harms for each product or service; (c) whether additional safeguards are available that could better mitigate the identified Privacy Risks and Harms or address any residual unresolved Privacy Risks and Harms; and (d) the sufficiency of any proposed User notice and, if necessary, consent; and

(ii) documenting the decision or recommendation made as a result of the review (e.g., whether the practice was approved, approved contingent upon safeguards or other recommendations being implemented, or rejected).

b. For each new or modified product, service, or practice that presents material Privacy Risks and Harms (e.g., a completely new product, service, or practice that has not been previously subject to Privacy Review, including any that result from a merger or Acquisition; a material change in the sharing of Covered Information with a Facebook-owned affiliate; a modified product, service, or practice that includes a material change in the collection, use, or sharing of Covered Information; a product, service, or practice directed to Children or Teens; or a product, service, or practice involving health, financial, biometric, or other similarly sensitive information), produce a written report ("Privacy Review Statement") that describes:

(i) The individual product, service, or feature thereof that presents material Privacy Risks and Harms, both on a standalone basis and within the context

of the broader product or service that it will be supporting or operating (e.g., considering the product or service inclusive of all relevant features);

(ii) The specific type(s) of Covered Information that will be collected, used, retained, or shared; how that Covered Information will be collected, used, retained, and shared; and an explanation for how collecting each type of Covered Information is necessary for providing the product or service to consumers;

(iii) The length of time that each type of Covered Information will be retained, and an explanation for why Respondent cannot retain the Covered Information for a shorter period of time;

(iv) The notice provided to Users about, and the mechanism(s), if any, by which Users will provide Affirmative Express Consent to, the collection of their Covered Information and the purposes for which such information will be used, retained, or shared by Respondent;

(v) A full description of the Privacy Risks and Harms associated with the product, service, or feature;

(vi) A full description of the safeguards, including:

(a) The existing and fully implemented safeguards that would control for the identified Privacy Risks and Harms;

(b) Any new safeguards needed to control for the identified Privacy Risks and Harms and the date when such safeguards will be fully implemented (not to exceed the date when the product or service is made available to consumers);

(c) The date, not to exceed sixty (60) days after the product or service is made available to consumers, that the implemented safeguard(s) will be evaluated for effectiveness in mitigating the identified Privacy Risks and Harms, and the criteria that will be used for this evaluation; and

(d) Once the safeguard evaluation is completed, the results of the evaluation and the date, not to exceed ninety (90) days after the product or service is made available to consumers, when any additional safeguards, if necessary, will be implemented to address any residual or other Privacy Risks and Harms; and

(vii) A full description of any residual Privacy Risks and Harms that were not mitigated by the safeguards described under subpart

VIII.E.2.b.(vi), and the reason(s) why no safeguards were implemented to mitigate those residual Privacy Risks and Harms.

c. Respondent must maintain a comprehensive list of any product or service changes and document whether each such product or service change underwent a Privacy Review. Such list(s) must include a description of the product or service change(s) and the reason(s) why the product change(s) did or did not merit a Privacy Review under the terms of subpart VIII.E.2 of this Order. This list is not required to include code fixes, third-party security vulnerabilities, or other changes that merely fix or improve existing code without changing the product or service.

d. The Designated Compliance Officer(s) shall deliver a quarterly report ("Quarterly Privacy Review Report") to the Principal Executive Officer and to the Assessor that provides: (i) a summary of the Privacy Review Statements generated during the prior fiscal quarter under subpart VIII.E.2.b, including a detailed discussion of the material risks to the privacy, confidentiality, security, and Integrity of the Covered Information that were identified and how such risks were addressed; (ii) an appendix with each Privacy Review Statement generated during the prior fiscal quarter under subpart VIII.E.2.b; and (iii) an appendix that lists all privacy decisions generated during the prior fiscal quarter under subpart VIII.E.2.a.

e. The appendices required under subpart VIII.E.2.d(ii) and (iii) shall be provided to the Assessor no fewer than twenty-one (21) days in advance of the quarterly meeting of the Independent Privacy Committee as specified in subpart XII.A.5. A copy of the summary in the Quarterly Privacy Review Report required under VIII.E.2.d(i) shall be provided to Assessor no fewer than fourteen (14) days in advance of the quarterly meeting; and

f. A copy of the Quarterly Privacy Review Report shall also be furnished, upon request, to the Commission.

3. Specifically with respect to Respondent's own employees' access to Covered Information, such safeguards shall include designing, implementing, and maintaining access policies and controls that limit employee access to any table(s) or other comparable data storage units known to contain Covered Information to only those employees with a business need to access such Covered Information.

4. Specifically with respect to Respondent's compliance with the Order in connection with a merger or Acquisition, such safeguards shall include designing, implementing, and maintaining policies to ensure that:

a. Any merged or acquired entity, talent, or data, or combination thereof, that becomes part of Meta Platforms, Inc. will comply with the terms of this Order as of the effective date of the merger or Acquisition;

b. Any merged or acquired entity, talent, or data, or combination thereof, that becomes an affiliate of Meta Platforms, Inc. will comply with the terms of this Order promptly, and in any event no later than forty-five (45) days after the effective date of that affiliate's merger or Acquisition; and

c. Any entity, talent, or data, or combination thereof, that has stronger privacy protections, policies, and practices than Respondent and becomes part of Meta Platforms, Inc. or an affiliate thereof maintains those stronger privacy protections, policies, and practices and continues to honor its prior Commitments to Users and/or consumers for a period of at least twelve (12) months.

5. Specifically with respect to facial recognition, such safeguards shall include:

a. Prior to using or sharing any Facial Recognition Template for a User in a manner that materially exceeds the types of uses or sharing disclosed to that User at the time that User's Affirmative Express Consent was previously obtained,

(i) Clearly and Conspicuously disclosing (such as in a stand-alone disclosure or notice), separate and apart from any "privacy policy," "data policy," "statement of rights and responsibilities" page, or other similar document, how Respondent will use or, to the extent applicable, share, such Facial Recognition Template; and

(ii) Obtaining the User's Affirmative Express Consent; and

b. Nothing in this provision shall limit Respondent's ability to use Facial Recognition Templates for fraud prevention or remediation, or for protecting the safety, reliability and security of Respondent's platform or Users, so long as Respondent discloses these types of uses in Respondent's privacy policy or similar document.

6. Specifically with respect to Respondent's management of Covered Information, such safeguards shall include:

a. Requiring Respondent maintain an inventory of all systems, products, and services that process, hold, or use Covered Information; and

b. Requiring Respondent maintain a description, including through graphic representation, of the architecture of the data centers, servers, databases, applications, or other places where Users' Covered Information is collected, received, used, processed, stored, or transferred.;

F. Assess, monitor, and test, at least once every twelve (12) months and promptly (not to exceed thirty (30) days) following the resolution of a Covered Incident, the effectiveness of any safeguards put in place pursuant to subpart VIII.E. of this Order to address the risks to the privacy,

confidentiality, security, or Integrity of Covered Information. Respondent shall modify the Mandated Privacy Program based on the results of this assessing, monitoring, and testing at least once every twelve (12) months and promptly (not to exceed sixty (60) days) following the resolution of a Covered Incident;

G. Implement and maintain the procedures necessary regarding the handling of Covered Information of Youth Users to comply with Part I of this Order;

H. Establish regular privacy training programs for all employees on at least an annual basis, updated to address any internal or external risks identified by Respondent in subpart VIII.D. of this Order and safeguards implemented pursuant to subpart VIII.E. of this Order. These training programs will include training on the requirements of this Order; an introduction to Privacy Risks and Harms and mitigation; and specific role-based training based on the employee's responsibilities under the Mandated Privacy Program. Any employee who has not completed the annual privacy training within the prior thirteen (13) months shall be denied access to Covered Information until such time as they complete the training;

I. Select and retain service providers capable of safeguarding Covered Information they receive from Respondent, and contractually require service providers to implement and maintain safeguards for Covered Information;

J. Consult with independent, third-party experts on data protection and privacy, and document the identity of all such experts and their recommendations or other guidance received in the course of establishing, implementing, maintaining, and updating the Mandated Privacy Program; and

K. Evaluate and adjust the Mandated Privacy Program in light of any material changes to Respondent's operations or business arrangements, a Covered Incident, new or more efficient technological or operational methods to control for the risks identified in subpart VIII.D. of this Order, and any other circumstances that Respondent knows or has reason to believe may have a material impact on the effectiveness of the Mandated Privacy Program. Respondent may make this evaluation and adjustment to the Mandated Privacy Program at any time, but must, at a minimum, evaluate the Mandated Privacy Program at least once every twelve (12) months and modify the Mandated Privacy Program as necessary based on the results.

IX. INDEPENDENT MANDATED PRIVACY PROGRAM ASSESSMENTS

IT IS FURTHER ORDERED that, in connection with compliance with Part VIII of this Order titled Mandated Privacy Program, Respondent must obtain initial and biennial assessments ("Assessments"):

A. The Assessment must be obtained from one or more qualified, objective, independent third-party professionals ("Assessor(s)"), selected by the Respondent, subject to the reasonable approval of the Independent Privacy Committee and subject to subpart IX.B, who: (1) uses procedures and standards generally accepted in the profession; (2) conducts an independent review of the Mandated Privacy Program; and (3) retains all documents relevant to each Assessment for five (5) years after completion of such Assessment and furnishes such documents

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

B. For each Assessment, Respondent must provide the Associate Director for Enforcement for the Bureau of Consumer Protection at the Federal Trade Commission ("Associate Director") with the name(s) and affiliation(s) of the person(s) selected to conduct the Assessment, which the Associate Director shall have the authority to approve in his or her sole discretion;

C. The reporting period for the Assessments must cover: (1) the first 180 days after the Mandated Privacy Program has been put in place for the initial Assessment; and (2) each two-year period thereafter for twenty (20) years after issuance of the Order for the biennial Assessments;

D. Each Assessment must: (1) determine whether Respondent has implemented and maintained the Mandated Privacy Program required by Part VIII of this Order, titled Mandated Privacy Program; (2) assess the effectiveness of Respondent's implementation and maintenance of each subpart in Part VIII of this Order; (3) identify any gaps or weaknesses in the Mandated Privacy Program; (4) identify specific evidence (including, but not limited to, documents reviewed, sampling and testing performed, and interviews conducted) examined to make such determinations, assessments, and identifications, and explain why the evidence that the Assessor examined is sufficient to justify the Assessor's findings; and (5) determine whether Respondent has implemented and maintained the procedures necessary regarding the handling of Covered Information of Youth Users to comply with Part I of this Order. To the extent that Respondent revises, updates, or adds one or more safeguards required under subpart VIII.E. of this Order in the middle of an Assessment period, the Assessment shall 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. Respondent and its Representatives must disclose all material facts to the Assessor(s), and must not misrepresent in any manner, expressly or by implication, any fact material to the Assessor(s)': (1) determination of whether Respondent has implemented and maintained the Mandated Privacy Program required by Part VIII of this Order; (2) assessment of the effectiveness of the implementation and maintenance of subparts VIII.A-K of this Order; or (3) identification of any gaps or weaknesses to the Mandated Privacy Program;

F. Respondent and its Representatives, whether acting directly or indirectly, must provide or otherwise make available to the Assessor all information and material in their possession, custody, or control that is relevant to the Assessment for which there is no reasonable claim of privilege;

G. No finding of any Assessment shall rely primarily on assertions or attestations by Respondent's management. The Assessment shall be signed by the Assessor and shall state that the Assessor conducted an independent review of the Mandated Privacy Program, and did not rely primarily on assertions or attestations by Respondent's management;

H. Each Assessment must be completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Unless otherwise directed by a Commission representative in writing, Respondent must submit each Assessment to the Commission within ten (10) days after the 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. The subject line must begin, "*In re Facebook, Inc.*, FTC File No. 182-3109." Each Assessment shall be retained by Respondent until this Order is terminated, and shall be provided to the Associate Director within ten (10) days of Request; and

I. The Assessor may only be removed by Respondent from such position, subject to subpart IX.B, with the affirmative vote of a majority of the Independent Privacy Committee.

X. VERIFICATION OF MANDATED PRIVACY PROGRAM COMPLIANCE BEFORE INTRODUCTION OF NEW OR MODIFIED PRODUCTS, SERVICES, OR FEATURES

IT IS FURTHER ORDERED that:

A. Prior to Respondent introducing any new or modified products, services, or features, the Assessor's most recent Assessment must show that Respondent's Mandated Privacy Program meets all the requirements of Part VIII, and the Assessor did not identify any material gaps or weaknesses in Respondent's Mandated Privacy Program.

B. If the most recent Assessment shows material gaps or weaknesses in Respondent's Mandated Privacy Program, Respondent may not introduce any new or modified products, services, or features, until the Assessor provides written confirmation to the Commission that Respondent has fully remediated all such material gaps and weaknesses.

C. However, subpart B does not restrict Respondent from introducing any new product or service for the sole purpose of protecting the privacy, confidentiality, security, or Integrity of Covered Information, as long as Respondent provides the Commission with a written description at least thirty (30) days in advance and the Assessor provides approval in writing for its release.

D. Nothing in this provision shall limit Respondent's ability to promptly address security vulnerabilities or implement code fixes that are necessary to maintain existing functionality and do not introduce new products or services.

XI. COVERED INCIDENT REPORTS

IT IS FURTHER ORDERED that Respondent must submit a report within thirty (30) days following Respondent's verification or confirmation of a Covered Incident, and subsequently updated every thirty (30) days until the Covered Incident is fully investigated and any remediation efforts are fully implemented, to the Assessor(s) and to the Commission, that includes, to the extent possible:

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

B. An overview of the facts relating to the Covered Incident, including the causes of the Covered Incident;

C. A description of each type of Covered Information that was accessed, collected, used, destroyed, or shared without the User's authorization or consent;

D. The number of Users whose Covered Information was accessed, collected, used, destroyed, or shared without the User's authorization or consent; and

E. An overview of the acts, if any, that Respondent has taken to date to remediate the Covered Incident and protect Covered Information from further exposure or access, including a description of any new safeguards that have been implemented in response to the Covered Incident.

Unless otherwise directed by a Commission representative in writing, all reports 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. The subject line must begin, "*In re Facebook, Inc.*, FTC File No. 182-3109." Within forty-five (45) days following Respondent's verification or confirmation of a Covered Incident, Respondent must publish on its website a public version of each Covered Incident report and maintain each report on its website for two (2) years.

XII. MANDATED INDEPENDENT PRIVACY COMMITTEE AND OTHER GOVERNANCE MATTERS

IT IS FURTHER ORDERED that:

A. Respondent shall maintain the Independent Privacy Committee responsible for monitoring and overseeing Respondent's compliance with this Order. Respondent shall further maintain the corporate charter for such committee that includes the following qualifications, authority, and responsibilities:

1. The committee shall hold at least four regularly scheduled meetings each year;

2. Each member of the committee shall be an Independent Director, and each of the members of the committee shall meet the Privacy and Compliance Baseline Requirements;

3. Each quarter, the Respondent shall cause the committee to receive a briefing from management regarding: (a) the state of the Mandated Privacy Program; (b) Respondent's compliance with the Order; and (c) material risks to the privacy, confidentiality, security, and Integrity of the Covered Information that have been discovered since the most recent meeting of the committee or that were raised by management in a prior meeting with the committee and continue to persist;

4. On at least an annual basis, management shall conduct a review for the committee of the Mandated Privacy Program and discuss Respondent's assessment of material risks to the privacy, confidentiality, security, and Integrity of the Covered Information and the steps Respondent has taken or plans to take to monitor or mitigate such risks, including Respondent's procedures and any related policies with respect to risk assessment and risk management;

5. The committee shall meet with the Assessor at least quarterly, and at the conclusion of each biennial Assessment;

a. At each quarterly meeting, the Assessor shall review with management and the committee: (i) the Assessor's ongoing assessment of the Mandated Privacy Program; and (ii) any material risks to the privacy, confidentiality, security, and Integrity of the Covered Information that have been identified by the Assessor since the Assessor's most recent meeting with the committee, or that were raised by the Assessor in a prior meeting with the committee and continue to persist;

b. At each quarterly meeting, the committee (together with any other Independent Directors in attendance) shall meet with the Assessor in an executive session without management present to discuss matters involving the Assessment or other privacy-related issues or risks, as appropriate; and

c. At the meeting to review the biennial Assessment with the Assessor, the Assessor and the committee shall review the various elements of the Assessment, as well as: (i) any material issues raised by the most recent Assessment or material unresolved issues from prior Assessments; and (ii) in an executive session without management present, any problems or difficulties with management. Following the review of the biennial Assessment (at either the same meeting or the following meeting), management shall review with the committee its proposed remediation plans to address any such issues raised in the Assessment;

6. The committee shall evaluate the independence of the Assessor, and the Assessor shall not be appointed or removed by Respondent, subject to Part IX.B, without the prior approval of a majority of the committee; and

7. Within forty-five (45) days after the end of the first full quarter after the effective date of this Order, and within forty-five (45) days after the end of each subsequent calendar quarter, the committee shall submit a written progress report to the Board of Directors setting forth in detail the actions taken to comply with each Part of this Order, and the results and status of those action.

B. Respondent shall maintain the Independent Nominating Committee, including the relevant committee charter providing that such committee shall have the following authority and responsibilities, including:

1. The committee shall have the sole authority to recommend the appointment of directors, or the nomination of candidates for election, to Respondent's Board of Directors, such that Respondent's Board of Directors may not approve any such appointment or

nomination in the absence of a favorable recommendation from the committee;

2. The committee shall have the sole authority to recommend the appointment of directors to, or the removal of directors from, the Independent Privacy Committee, such that Respondent's Board of Directors may not approve any such appointment or removal in the absence of a favorable recommendation from the committee; and

3. The committee shall determine whether the members of the Independent Privacy Committee qualify as Independent Directors and whether each member of the Independent Privacy Committee meets the Privacy and Compliance Baseline Requirements and whether the composition of the Independent Privacy Committee satisfies the requirements set forth in Definition M of this Order. The foregoing determinations shall be made prior to, or concurrent with, the formation of the Independent Privacy Committee for the initial members; and prior to, or concurrent with, the appointment of each new director to the Independent Privacy Committee for future members.

C. For the duration of this Order, Respondent shall not alter or amend the 2020 amendment to Article VI, Section 4, of Respondent's Certificate of Incorporation, which added a new Article VI, Section 4(b) with respect to the removal of directors, .; and

D. Nothing in this Order shall be construed to expand, modify, or alter the fiduciary duties of the members of the Respondent's Board of Directors or any committee thereof.

XIII. CERTIFICATIONS

IT IS FURTHER ORDERED that Respondent shall:

A. Within forty-five (45) days after the end of each full fiscal quarter (but in no event later than the first meeting of the Independent Privacy Committee with respect to such fiscal quarter (as provided in subpart XII.A)) following the anniversary of the effective date of this Order, provide the Commission with its certification, signed by the Principal Executive Officer and the Designated Compliance Officer(s) on behalf of Respondent, that, with respect to such fiscal quarter: (1) Respondent has established, implemented, and maintained a Mandated Privacy Program that complies in all material respects with the requirements of Part VIII of this Order; and (2) Respondent is not aware of any material noncompliance with Part IX that has not been corrected or disclosed to the Commission. In making this certification on behalf of Respondent, the Principal Executive Officer shall rely, and be entitled to rely, solely on the following: (1) his or her personal knowledge; (2) sub-certifications regarding compliance with Part IX, provided by knowledgeable personnel charged with implementing the Mandated Privacy Program; and (3) the Principal Executive Officer's review of the summaries in the Quarterly Privacy Review Report required under Part IX.E.2.d(i) for such fiscal quarter, as well as any material issues raised in Covered Incident Reports required under Part IX for such fiscal quarter. The Designated Compliance Officer(s) shall rely, and be entitled to rely, solely on the following: (1) his or her personal knowledge; (2) sub-certifications regarding compliance with Part VIII, provided by knowledgeable personnel charged with implementing the Mandated Privacy Program; (3) material issues identified in the Quarterly Privacy Review Report required under Part VIII.E.2.d.; and (4) material issues raised in the Covered Incident Reports required under Part XI for such fiscal

quarter. Within fourteen (14) days of submitting its certification to the Commission, Respondent must publish on its website a public version of the certification and maintain each certification on its website for two (2) years; and

B. Within forty-five (45) days after the end of the first full fiscal quarter (but in no event later than the first meeting of the Independent Privacy Committee with respect to such fiscal quarter (as provided in Part XII.A.)) following the anniversary of the effective date of this Order and every year thereafter, provide the Commission with its certification, signed by the Principal Executive Officer and the Designated Compliance Officer(s) on behalf of Respondent, that: (1) Respondent has established, implemented, and maintained the requirements of this Order in all material respects; and (2) Respondent is not aware of any material noncompliance with this Order that has not been corrected or disclosed to the Commission. In making this certification on behalf of Respondent, the Principal Executive Officer shall rely, and be entitled to rely, solely on the following: (1) his or her personal knowledge; (2) sub-certifications regarding compliance with Part VIII of this Order, provided by knowledgeable personnel charged with implementing the Mandated Privacy Program; and (3) the Principal Executive Officer's review of the written program required under subpart VIII.A. of this Order and the summaries in the Quarterly Privacy Review Reports required under subpart VIII.E.2.d(i) for the preceding year, as well as any material issues raised in Covered Incident Reports required under Part IX for the preceding year. The Designated Compliance Officer(s) shall rely, and be entitled to rely, solely on the following: (1) his or her personal knowledge; (2) sub-certifications regarding compliance with Part IX, provided by knowledgeable personnel charged with implementing the Mandated Privacy Program; (3) material issues identified in the Quarterly Privacy Review Reports required under Part IX.E.2.d. for the preceding year; and (4) material issues raised in the Covered Incident Reports required under Part XI for the preceding year. Within fourteen (14) days of submitting its certification to the Commission, Respondent must publish on its website a public version of the certification and maintain each certification on its website for two (2) years.

Unless otherwise directed by a Commission representative in writing, Respondent shall submit all 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. The subject line must begin, "*In re Facebook, Inc*., FTC File No. 182-3109."

XIV. ORDER ACKNOWLEDGMENTS

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

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

B. For five (5) years after entry of this Order, Respondent must deliver a copy of this Order to: (1) all principals, officers, directors, and LLC managers and members; (2) all employees having managerial responsibilities for conduct related to the subject matter of the Order and all agents and representatives who participate in 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 Part titled Compliance Reporting (Part XV). Delivery must occur within seven (7) days of entry of this Order for current personnel. For all others, delivery must occur before they assume their responsibilities; and

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

XV. COMPLIANCE REPORTING

IT IS FURTHER ORDERED that Respondent make timely submissions to the Commission:

A. One hundred eighty (180) days after entry of this Order, Respondent must submit a compliance report, sworn under penalty of perjury, which: (1) identifies the primary physical, postal, and email address and telephone number, as designated points of contact, which representatives of the Commission may use to communicate with Respondent; (2) identifies all of Respondent's businesses by all of their names, telephone numbers, and physical, postal, email, and Internet addresses; (3) describes the activities of each business; (4) describes in detail whether and how Respondent is in compliance with each Part of this Order; and (5) provides a copy of each Order Acknowledgment obtained pursuant to this Order, unless previously submitted to the Commission;

B. For twenty (20) years after entry of this Order, Respondent must submit a compliance notice, sworn under penalty of perjury, within fourteen (14) days of any change in the following: (1) any designated point of contact; (2) Respondent's corporate structure; or (3) the structure of any entity that Respondent 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. Respondent must submit to the Commission notice of the filing of any bankruptcy petition, insolvency proceeding, or similar proceeding by or against Respondent within fourteen (14) days of its filing;

D. Any submission to the Commission 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, to the best of my knowledge and reasonable belief, the foregoing is true and correct. Executed on: _____" and supplying the date, signatory's full name, title (if applicable), and signature; and

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.

The subject line must begin: "*In re Facebook, Inc.*, FTC File No. 182-3109."

XVI. RECORDKEEPING

IT IS FURTHER ORDERED that Respondent must create certain records for twenty (20) years after entry of the Order and retain each such record for five (5) years. Specifically, Respondent must create and retain the following records:

A. All widely disseminated statements by Respondent or its Representatives that describe the extent to which Respondent maintains and protects the privacy, security, confidentiality and Integrity of any Covered Information, including, but not limited to, any statement related to a change in any website or service controlled by Respondent that relates to the privacy of such information, along with all materials relied upon in making such statements, and a copy of each materially different Privacy Setting made available to Users (including screenshots/screencasts of Privacy Settings and the User interfaces, consent flows, and paths a User must take to reach such settings);

B. Records sufficient to identify the types of Covered Information that Respondent provides or makes available to any Covered Third Party that is subject to the requirements of subpart VIII.E.1, including records identifying: (1) the specific data fields to which access was granted; (2) the means by which the information was provided or made available; (3) the identity of the Covered Third Party to which access was granted; (4) the self-certifications provided by the Covered Third Party (as described in subpart VIII.E.1); and (5) the date(s) when access was provided;

C. All consumer complaints directed at Respondent or forwarded to Respondent by a Covered Third Party that relate to the conduct prohibited by this Order and any responses to such complaints;

D. Records sufficient to identify the procedures and processes for handling Covered Information for Youth Users that are subject to the requirements of Part I;

E. Any documents, prepared by or on behalf of Respondent, that contradict, qualify, or call into question Respondent's compliance with this Order;

F. Each materially different document relating to Respondent's attempt to obtain the consent of Users referred to in Part III titled Changes To Sharing Of Nonpublic User Information, along with documents and information sufficient to show each User's consent; and documents sufficient to demonstrate, on an aggregate basis, the number of Users for whom each such Privacy Setting was in effect at any time Respondent has attempted to obtain and/or been required to obtain such consent;

G. All materials relied upon to prepare the Assessment, whether prepared by or on behalf of Respondent, including but not limited to all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, for the compliance period covered by such Assessment; and

H. All records necessary to demonstrate full compliance with each Part of this Order, including all submissions to the Commission.

XVII. COMPLIANCE MONITORING

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

A. Within fourteen (14) days of receipt of a written request from a representative of the Commission, Respondent 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 is 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 telephonic depositions), 31, 33, 34, 36, 45, and 69;

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

C. The Commission may use all other lawful means, including posing, through its representatives, as consumers, suppliers, or other individuals or entities, to Respondent or any individual or entity affiliated with Respondent, 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.

XVIII. ORDER EFFECTIVE DATES

IT IS FURTHER ORDERED that this Order is final and effective upon the date of its publication on the Commission's website (ftc.gov) as a final order. This Order will terminate 20 years from the date of its issuance, or 20 years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying settlement) in federal court alleging any violation of this Order, whichever comes later; *provided, however,* that the filing of such a complaint will not affect the duration of:

A. Any Part in this Order that terminates in less than 20 years;

B. This Order's application to any Respondent that is not named as a defendant in such complaint; and

C. This Order if such complaint is filed after the Order has terminated pursuant to this Part.

Provided, further, that if such complaint is dismissed or a federal court rules that the Respondent did not violate any Part of the Order, and the dismissal or ruling is either not appealed or upheld on appeal, then the Order will terminate according to this Part as though the complaint had never

been filed, except that the Order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

April Tabor
Secretary

SEAL:
ISSUED: