

COPY

XAVIER BECERRA
Attorney General of California
NICKLAS A. AKERS
Senior Assistant Attorney General
STACEY D. SCHESSER
Supervising Deputy Attorney General
YEN P. NGUYEN (SBN 239095)
Deputy Attorney General
455 Golden Gate Avenue, Suite 11000
San Francisco, CA 94102-7004
Telephone: (415) 510-3497
Fax: (415) 703-5480
E-mail: TiTi.Nguyen@doj.ca.gov

Attorneys for The People of the State of California

SUPERIOR COURT OF THE STATE OF CALIFORNIA

FOR THE COUNTY OF SAN FRANCISCO

UNLIMITED JURISDICTION

[EXEMPT FROM FILING FEES
PURSUANT TO GOVERNMENT
CODE SECTION 6103]

ENDORSED
FILED
San Francisco County Superior Court
SEP 17 2020
CLERK OF THE COURT
BY: EDWARD SANTOS
Deputy Clerk

THE PEOPLE OF THE STATE OF
CALIFORNIA,

Plaintiff,

v.

UPWARD LABS HOLDINGS, INC., a
corporation, and GLOW, INC., a
corporation,

Defendants.

Case No.

CGC-20-586611

STIPULATION FOR ENTRY OF FINAL
JUDGMENT AND PERMANENT
INJUNCTION

(CIVIL CODE, §§ 56.06(b), 56.101, 56.10(a);
BUS. & PROF., §§ 17200 *et seq.*, 17500 *et seq.*)

Plaintiff, the People of the State of California ("the People" or "Plaintiff"), appearing through its attorney, Xavier Becerra, Attorney General of the State of California, by Yen P. Nguyen, Deputy Attorney General, and Stacey D. Schesser, Supervising Deputy Attorney General, and Defendants Upward Labs Holdings, Inc. and Glow, Inc., both corporations ("Defendants"), appearing through their attorney, Matthew D. Brown of Cooley LLP, stipulate as follows:

1 1. The Court has jurisdiction of the subject matter hereof and the parties to this
2 Stipulation for Entry of Final Judgment and Permanent Injunction (“Stipulation”).

3 2. Concurrently with the filing of this Stipulation, Plaintiff has filed its Complaint in
4 this matter alleging that Defendant committed violations of Civil Code sections 56.06(b),
5 56.10(a), and 56.101 and Business and Professions Code sections 17200 et seq. and 17500 et seq.

6 3. The Final Judgment and Permanent Injunction (“Final Judgment”), a true and
7 correct copy of which is attached hereto as Exhibit A, may be entered by any judge of the San
8 Francisco County Superior Court.

9 4. Plaintiff and Defendants (collectively, “the Parties”) have agreed to resolve these
10 allegations contained in the Plaintiff’s Complaint by entering into this Stipulation.

11 5. Plaintiff and Defendants (collectively, “the Parties”) hereby waive their right to
12 move for a new trial or otherwise seek to set aside the Final Judgment through any collateral
13 attack, and further waive their right to appeal from the Final Judgment, except that Plaintiff and
14 Defendant each agree that this Court shall retain jurisdiction for the purposes specified in
15 Paragraph 40 of the Final Judgment.

16 6. This Stipulated Judgment shall have res judicata effect and shall bar any action by
17 Plaintiff, the People of the State of California, against (a) Defendants, (b) their directors, officers,
18 employees, and agents acting within their capacities as such, (c) their subsidiaries, and (d) their
19 successors and the assigns of all or substantially all of the assets of their businesses, from all civil
20 claims alleged in the Complaint and any and all civil claims that could have been brought,
21 including but not limited to claims under Business and Professions Code sections 17200 et seq.,
22 17500 et seq., and 22575 et seq. and Civil Code sections 56 et seq. and 1798.81.5 relating to
23 Defendants’ acts or omissions through the entry of the Final Judgment related to the privacy or
24 security of their mobile applications or online services. Nothing contained in this Paragraph shall
25 be construed to limit the ability of the Attorney General to enforce the obligations that Defendants
26 have under the Judgment.

27 7. The Parties have stipulated and consented to the entry of the Final Judgment
28 without the taking of proof and without trial or adjudication of any fact or law herein, without the

1 Final Judgment constituting evidence or an admission or concession by Defendants regarding any
2 claim or issue of law or fact alleged in the Complaint on file herein or within the scope of the
3 Final Judgment, and without Defendants admitting or conceding any liability or wrongdoing
4 regarding acts or omissions or alleged legal violations that occurred or allegedly occurred prior to
5 the entry of the Final Judgment. In stipulating to the entry of the Final Judgment, Defendants do
6 not intend to create any legal or voluntary standard of care and expressly deny that any practices,
7 policies, or procedures inconsistent with those set forth in the Final Judgment violate any
8 applicable legal standard.

9 8. Plaintiff may submit the Final Judgment to any judge of the superior court for
10 approval and signature, based on this stipulation, during the court's *ex parte* calendar or on any
11 other *ex parte* basis, without notice to or any appearance by Defendants which notice and right to
12 appear Defendants hereby waive.

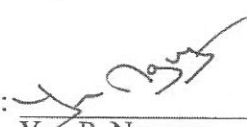
13 9. Defendants will accept service of any Notice of Entry of Judgment entered in this
14 action by delivery of such notice to their counsel of record, and agree that service of the Notice of
15 Entry of Judgment will be deemed personal service upon them for all purposes.

16 10. The individuals signing below represent that they have been authorized by the
17 parties they represent to sign this Stipulation.

18 11. This Stipulation may be executed in counterparts, and the Parties agree that a
19 facsimile, scanned, or electronic signature shall be deemed to be, and shall have the full force and
20 effect as, an original signature.

21
22 Dated: September 14, 2020

XAVIER BECERRA
Attorney General of California

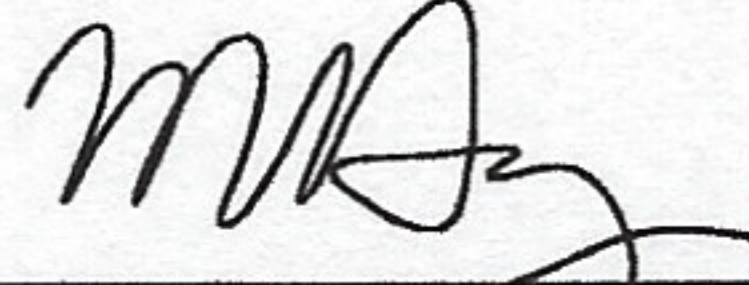
23
24
25 BY: 
26 Yen P. Nguyen
27 Deputy Attorney General
28 Attorneys for Plaintiff

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Dated: September 10, 2020

Dated: September 10, 2020

UPWARD LABS HOLDINGS, INC. AND GLOW,
INC.

BY: 
NAME Michael Huang
TITLE President
ADDRESS 499 Jackson Street, 3rd Floor
San Francisco, CA 94111

COOLEY LLP

BY: 
Matthew D. Brown, SBN 196972
COOLEY LLP
101 California St., Fifth Floor
San Francisco, CA 94111
Tel.: (415) 693-2188
Fax: (415) 693-2222
brownmd@cooley.com
Attorney for Defendants

EXHIBIT A

XAVIER BECERRA
Attorney General of California
NICKLAS A. AKERS
Senior Assistant Attorney General
STACEY D. SCHESSER
Supervising Deputy Attorney General
YEN P. NGUYEN (SBN 239095)
Deputy Attorney General
455 Golden Gate Avenue, Suite 11000
San Francisco, CA 94102-7004
Telephone: (415) 510-3497
Fax: (415) 703-5480
E-mail: TiTi.Nguyen@doj.ca.gov

Attorneys for The People of the State of California

SUPERIOR COURT OF THE STATE OF CALIFORNIA

FOR THE COUNTY OF SAN FRANCISCO

UNLIMITED JURISDICTION

**PEOPLE OF THE STATE OF
CALIFORNIA,**

Plaintiff,

v.

**UPWARD LABS HOLDINGS, INC., a
corporation, and GLOW, INC., a
corporation,**

Defendants.

Case No.

**[PROPOSED] FINAL JUDGMENT AND
PERMANENT INJUNCTION**

Plaintiff, the People of the State of California (“the People” or “Plaintiff”), appearing through its attorney, Xavier Becerra, Attorney General of the State of California, by Yen P. Nguyen, Deputy Attorney General, and Stacey D. Schesser, Supervising Deputy Attorney General, and Defendants Upward Labs Holdings, Inc. and Glow, Inc., both corporations (“Defendants”), appearing through their attorney, Matthew D. Brown of Cooley LLP, having stipulated to the entry of this Final Judgment and Permanent Injunction (“Judgment”) by the Court without the taking of proof and without trial or adjudication of any fact or law, without this Judgment constituting evidence of or an admission by Upward Labs Holdings, Inc. or Glow, Inc.

1 regarding any issue or law or fact alleged in the Complaint on file, and without Upward Labs
2 Holdings, Inc. or Glow, Inc. admitting any liability, and with all parties having waived their right
3 to appeal, and the Court having considered the matter and good cause appearing:

4 IT IS HEREBY ORDERED, ADJUDGED, AND DECREED THAT:

5 **I. PARTIES AND JURISDICTION**

6 1. This Court has jurisdiction over the allegations and subject matter of the People's
7 Complaint filed in this action, and the parties to this action; venue is proper in this County; and
8 this Court has jurisdiction to enter this Judgment.

9 **II. DEFINITIONS**

10 The following terms in this Judgment shall have these meanings:

11 2. "AFFIRMATIVE AUTHORIZATION" means an action that demonstrates the
12 intentional decision by the CONSUMER to authorize a request. Silence, pre-checked boxes,
13 inactivity, or responses obtained from a user interface designed to mislead or steer a user into an
14 unintended decision do not constitute AFFIRMATIVE AUTHORIZATION. A user's consent to
15 provisions in GLOW's terms of service or privacy policy may constitute AFFIRMATIVE
16 AUTHORIZATION if GLOW's method to obtain the user's consent complies with this definition
17 of AFFIRMATIVE AUTHORIZATION.

18 3. "CONSUMER" shall mean a user or consumer of any GLOW product or service.

19 4. "DEFENDANTS" or "GLOW" shall mean Upward Labs Holdings Inc. and Glow
20 Inc.

21 5. "EFFECTIVE DATE" shall mean the date this Judgment is entered.

22 6. "MEDICAL INFORMATION" shall include the meanings of "medical
23 information" as provided in the Confidentiality of Medical Information Act (CMIA), Civil Code
24 section 56 et seq., and the Data Security Law, Civil Code section 1798.81.5. Information is
25 "medical information" within the Confidentiality of Medical Information Act (CMIA), Civil
26 Code section 56 et seq., and the Data Security Law, Civil Code section 1798.81.5, irrespective of
27 how the information is transmitted, which may include the CONSUMER manually entering or
28 uploading the information into a mobile application or online service.

1 7. “PERSONAL INFORMATION” shall have the same meaning as provided in the
2 Data Security Law, Civil Code section 1798.81.5, with the exception of “medical information” as
3 defined in that code section.

4 8. “PERSONALLY IDENTIFIABLE INFORMATION” shall have the same
5 meaning as provided in the California Online Privacy Protection Act (CalOPPA), Business and
6 Professions Code section 22575 et seq.

7 9. “SENSITIVE PERSONAL DATA” shall mean information that is neither
8 MEDICAL INFORMATION nor PERSONAL INFORMATION but describes a CONSUMER’S
9 sexual activity, sexual health, and reproductive health and is collected, stored, processed, used,
10 transmitted, and/or maintained in an individually identifiable form.

11 **III. INJUNCTIVE PROVISIONS**

12 10. Nothing in this Judgment alters the requirements of state or federal law to the
13 extent they offer greater protection to CONSUMERS.

14 11. The injunctive provisions of this Judgment shall apply to: (a) DEFENDANTS; (b)
15 their directors, officers, employees, and agents acting within their capacities as such; (c) their
16 subsidiaries; and (d) their successors and the assigns of all or substantially all of the assets of their
17 businesses.

18 12. The injunctive terms contained in this Judgment are being entered pursuant to
19 Business and Professions Code section 17203.

20 **COMPLIANCE WITH LAW**

21 13. DEFENDANTS shall comply, to the extent applicable, with Civil Code sections
22 56.06, 56.10, 56.101, and 1798.81.5; Business and Professions Code sections 22575-22577;
23 Business and Professions Code section 17200, including in connection with its collection,
24 maintenance, and safeguarding of MEDICAL INFORMATION and PERSONAL
25 INFORMATION and its preservation of the confidentiality of MEDICAL INFORMATION; and
26 Business and Professions Code section 17500, including the extent to which they represent how
27 they maintain and/or protect the privacy, security, confidentiality, or integrity of any MEDICAL
28

1 INFORMATION, PERSONAL INFORMATION, or PERSONALLY IDENTIFIABLE
2 INFORMATION collected from or about CONSUMERS.

3 INFORMATION SECURITY PROGRAM

4 14. Within one hundred and eighty (180) days after the Effective Date, GLOW shall
5 implement, and thereafter shall maintain, regularly review and revise, and comply with an
6 information security program (“Information Security Program”) designed to protect the security,
7 integrity, availability,¹ and confidentiality of the PERSONAL INFORMATION, MEDICAL
8 INFORMATION, and SENSITIVE PERSONAL DATA that GLOW collects, stores, processes,
9 uses, transmits, and/or maintains.

10 15. GLOW’s Information Security Program shall be documented and shall contain
11 administrative, technical, and physical safeguards appropriate to:

12 a. The size and complexity of GLOW’s operations;
13 b. The nature and scope of GLOW’s activities; and
14 c. The sensitivity of the PERSONAL INFORMATION, MEDICAL
15 INFORMATION and SENSITIVE PERSONAL DATA that GLOW collects, stores, processes,
16 uses, transmits, and/or maintains.

17 16. The Information Security Program shall be designed to:

18 a. Protect the security, integrity, availability, and confidentiality of
19 PERSONAL INFORMATION, MEDICAL INFORMATION, and SENSITIVE PERSONAL
20 DATA;
21 b. Protect against credible threats that are known or reasonably foreseeable to
22 the security, integrity, availability, or confidentiality of PERSONAL INFORMATION,
23 MEDICAL INFORMATION, and SENSITIVE PERSONAL DATA;
24 c. Protect against unauthorized access to or use of PERSONAL
25 INFORMATION, MEDICAL INFORMATION, and SENSITIVE PERSONAL DATA;

26 _____
27 ¹ “Availability” means that the information is accessible and usable within a reasonable
28 timeframe upon demand by an authorized person. This does not include GLOW’s intentional
limitation on the availability of the information, such as for purposes of performing maintenance
or eliminating a feature in GLOW’s mobile application(s) or online service(s).

1 d. Protect against unauthorized disclosure of PERSONAL INFORMATION,
2 MEDICAL INFORMATION, and SENSITIVE PERSONAL DATA taking into account that
3 unauthorized disclosure includes unauthorized release to a location where such information is
4 readily accessible to an unauthorized party and does not require that an unauthorized party view
5 or read the information;

6 e. Implement reasonable authentication procedures prior to changing or
7 resetting a password, which, at a minimum, require two-factor authentication (i.e., requiring more
8 than just knowledge of a single password);

9 f. Obtain AFFIRMATIVE AUTHORIZATION to share or disclose
10 PERSONAL INFORMATION, MEDICAL INFORMATION, and SENSITIVE PERSONAL
11 DATA prior to sharing or disclosing such information with anyone outside of GLOW or its
12 service providers, except as required by law.

13 g. Obtain AFFIRMATIVE AUTHORIZATION to existing, ongoing, and/or
14 new use of MEDICAL INFORMATION for a purpose that is materially different from the
15 purposes disclosed to or understood by the CONSUMER at or before the time of collection of
16 such MEDICAL INFORMATION or that is not reasonably necessary for providing or facilitating
17 the intended functions or benefits of the mobile application or online service.

18 h. Restrict access to PERSONAL INFORMATION, MEDICAL
19 INFORMATION, and SENSITIVE PERSONAL DATA within GLOW based on necessity and
20 job function;

21 i. Accurately and thoroughly assess the potential risks and vulnerabilities to
22 the security, integrity, availability, and confidentiality of PERSONAL INFORMATION,
23 MEDICAL INFORMATION, and SENSITIVE PERSONAL DATA;

24 j. Assess the sufficiency and effectiveness of any safeguards in place to
25 control the risks and vulnerabilities identified in subsection (i);

26 k. Adjust these safeguards and the Information Security Program in light of
27 the results of the assessments in subsections (i) and (j); and
28

1 1. Provide employee training, on an ongoing basis at least annually,
2 concerning the proper handling and protection of PERSONAL INFORMATION, MEDICAL
3 INFORMATION, and SENSITIVE PERSONAL DATA.

4 17. GLOW may satisfy the implementation and maintenance of the Information
5 Security Program and the safeguards required by this Judgment through review, maintenance,
6 and, if necessary, updating, of an existing information security program or existing safeguards,
7 providing that such existing safeguards meet the requirements set forth in this Judgment.

8 18. Within ninety (90) days after the Effective Date, GLOW shall designate one or
9 more individuals employed or engaged by GLOW who shall make good-faith efforts to:

10 a. Be or become knowledgeable of relevant and applicable state and federal
11 privacy and data security statutes;

12 b. Ensure GLOW develops, implements, and maintains privacy and security
13 policies and procedures for GLOW that are consistent with applicable state and federal privacy
14 laws;

15 c. Be or become knowledgeable of Privacy-by-Design and Security-by-
16 Design principles;

17 d. Oversee GLOW's compliance with such policies and procedures; and

18 e. Oversee the implementation, maintenance, and monitoring of the
19 Information Security Program.

20 Such employee or employees, in their capacity as the person or persons with these
21 responsibilities, shall have authority and autonomy to perform these responsibilities and to report
22 any significant privacy or security concerns to the Chief Executive Officer or other GLOW
23 executives.

24 19. GLOW shall notify the California Attorney General's Office of the title(s) and
25 number of employees who have been designated pursuant to Paragraph 18 within thirty (30) days
26 after the deadline specified in Paragraph 18.

27 20. GLOW shall ensure that the Information Security Program receives reasonable
28 resources for carrying out the Information Security Program.

SPECIFIC SAFEGUARDS AND CONTROLS

21. GLOW shall conduct a regular inventory of its mobile applications and online services and document whether such application or service (i) is designed to maintain MEDICAL INFORMATION and/or (ii) collects, stores, processes, uses, transmits, and/or maintains PERSONAL INFORMATION, MEDICAL INFORMATION, and/or SENSITIVE PERSONAL DATA.

22. Any mobile application or online service offered by GLOW which (i) is designed to maintain MEDICAL INFORMATION and/or (ii) collects, stores, processes, uses, transmits, and/or maintains MEDICAL INFORMATION shall comply with the requirements of the Information Security Program set forth in Paragraphs 15-16 above.

23. Upon implementation of the Information Security Program pursuant to Paragraph 14, GLOW shall implement and maintain reasonable security procedures and practices designed to protect the PERSONAL INFORMATION, “medical information” as defined in the Data Security Law, Civil Code section 1798.81.5, and/or SENSITIVE PERSONAL DATA collected, stored, processed, used, transmitted, and/or maintained by any mobile application or online service offered by GLOW from unauthorized access, destruction, use, modification, or disclosure.

24. **AFFIRMATIVE AUTHORIZATION for Sharing or Disclosing CONSUMER Data:** Beginning no later than ninety (90) days after the Effective Date, GLOW shall obtain AFFIRMATIVE AUTHORIZATION from a CONSUMER before GLOW shares or discloses that CONSUMER’s PERSONAL INFORMATION, MEDICAL INFORMATION, or SENSITIVE PERSONAL DATA with any third-party person or entity outside of GLOW or its service providers, except as required by law. GLOW’s process for obtaining a CONSUMER’s AFFIRMATIVE AUTHORIZATION as required by the preceding sentence shall include, at a minimum:

a. A notice that is easy to read and understandable to a CONSUMER, and must, at the least, contain the following elements:

i. A description of the information that will be shared or disclosed;

ii. The name of the person or entity with whom the information will be shared or disclosed, or the category of such person or entity described with enough particularity to provide consumers with a meaningful understanding of the type of person or entity; and

iii. A description of the purpose for the disclosure.

b. A mechanism for the CONSUMER to provide AFFIRMATIVE AUTHORIZATION to the sharing or disclosure.

c. Making a record of the date the CONSUMER provided the AFFIRMATIVE AUTHORIZATION.

25. **AFFIRMATIVE AUTHORIZATION for Existing, Ongoing, and/or New Use of MEDICAL INFORMATION:** Beginning no later than ninety (90) days after the Effective Date, GLOW shall obtain AFFIRMATIVE AUTHORIZATION from a CONSUMER before GLOW uses that CONSUMER's MEDICAL INFORMATION for a purpose that is materially different from the purposes disclosed to or understood by the CONSUMER at or before the time of collection of such MEDICAL INFORMATION or that is not reasonably necessary for providing or facilitating the intended functions or benefits of the mobile application or online service. GLOW's process for obtaining a CONSUMER's AFFIRMATIVE AUTHORIZATION for such use of MEDICAL INFORMATION as required by the preceding sentence shall include, at a minimum:

a. A notice that is easy to read and understandable to a CONSUMER, and must, at the least, contain the following elements:

i. A description of the information that will be used;

ii. A description of the purpose for the use.

b. A mechanism for the CONSUMER to provide AFFIRMATIVE AUTHORIZATION to the sharing or disclosure.

c. Making a record of the date the CONSUMER provided the AFFIRMATIVE AUTHORIZATION.

26. **Revoking AFFIRMATIVE AUTHORIZATION:** Beginning no later than ninety (90) days after the Effective Date, GLOW shall allow a CONSUMER to revoke any

1 previously granted AFFIRMATIVE AUTHORIZATION required by Paragraphs 24 and 25 at any
2 time and shall process such revocations within a reasonably prompt timeframe after GLOW
3 receives them, and it shall not be a violation of this Judgment for GLOW to rely on the
4 previously-granted AFFIRMATIVE AUTHORIZATION until the revocation is processed.
5 GLOW shall accept requests for revocation submitted via email to one or more addresses
6 specified by GLOW in the notices described in Paragraphs 24(a) and 25(a). GLOW shall include
7 instructions on how a CONSUMER may revoke any previously granted AFFIRMATIVE
8 AUTHORIZATION in the notice referenced in Paragraphs 24 and 25.

9 27. GLOW may not condition use of any GLOW mobile application or online service
10 that (i) is designed to maintain MEDICAL INFORMATION and/or (ii) collects, stores, processes,
11 uses, transmits, and/or maintains PERSONAL INFORMATION, MEDICAL INFORMATION,
12 and/or SENSITIVE PERSONAL DATA on whether the CONSUMER: (a) provides an
13 AFFIRMATIVE AUTHORIZATION required by Paragraphs 24 or 25; or (b) revokes previously-
14 granted AFFIRMATIVE AUTHORIZATIONS, unless the information is reasonably required in
15 order for the feature in the mobile application or online service to function as intended.
16 Notwithstanding the foregoing, GLOW may charge a CONSUMER a different price or rate for
17 goods or services, or provide a different level of quality of goods or services to the CONSUMER,
18 if that price or difference is directly related to the value to provide to GLOW by the MEDICAL
19 INFORMATION, PERSONAL INFORMATION, or SENSITIVE PERSONAL DATA that
20 GLOW is unable to share or use as a result of the CONSUMER's election not to provide, or to
21 revoke, an AFFIRMATIVE AUTHORIZATION. Requiring an AFFIRMATIVE
22 AUTHORIZATION described in Paragraphs 24 and 25 as a condition of use of a GLOW online
23 service or mobile application shall not violate this Paragraph 27 so long as the CONSUMER may
24 revoke such AFFIRMATIVE AUTHORIZATION as described in Paragraph 27(27).

25 28. **Authenticating for Password Change or Reset:** When GLOW receives a
26 request from a CONSUMER of GLOW's mobile applications or online services to change or
27 reset his/her password, GLOW shall authenticate the CONSUMER prior to changing or resetting
28 the password, which, at a minimum, shall include two-factor authentication (i.e., requiring more

1 than just knowledge of a single password). Following a password change or reset, GLOW shall
2 require the CONSUMER to log into any GLOW mobile application or online service using the
3 new password.

4 **29. Application of Vulnerability Fixes:** Beginning no later than ninety (90) days
5 after the Effective Date, whenever GLOW patches a known security vulnerability in any mobile
6 application or online service offered by GLOW that materially impacts the security of a
7 CONSUMER's MEDICAL INFORMATION, PERSONAL INFORMATION, OR SENSITIVE
8 PERSONAL INFORMATION, GLOW shall require the CONSUMER to re-authenticate or go
9 through any new or additional security control added by the fix before using the mobile
10 application or online service. To the extent the vulnerability patch would require the
11 CONSUMER to download the revised mobile application or online service, GLOW shall use
12 commercially reasonable efforts to encourage CONSUMERS to download the revised mobile
13 application or online service.

14 **30. Privacy-by-Design and Security-by-Design:** No later than one hundred eighty
15 (180) days after the Effective Date, GLOW shall develop, implement, and maintain a process to
16 incorporate privacy-by-design principles and security-by-design principles, when:

17 a. Creating or developing any new GLOW mobile application or online
18 service which (i) is designed to maintain MEDICAL INFORMATION and/or (ii) collects, stores,
19 processes, uses, transmits, and/or maintains PERSONAL INFORMATION, MEDICAL
20 INFORMATION, and/or SENSITIVE PERSONAL DATA; or

21 b. Reviewing proposed changes to any feature of a GLOW mobile application
22 or online service that materially impacts the security of the manner in which a CONSUMER'S
23 MEDICAL INFORMATION, PERSONAL INFORMATION, or SENSITIVE PERSONAL
24 DATA is collected, stored, processed, used, transmitted, and/or maintained.

25 This process shall also be documented for review by the Attorney General. To the extent that any
26 existing or new GLOW mobile application is designed to be used primarily by CONSUMERS
27 who are women, this process of incorporating the privacy-by-design and security-by-design
28 principles shall consider how privacy or security lapses may impact online threats affecting

women and online risks that women face, or could face, including gender-based risks, from privacy and security lapses.

31. **Cyberstalking Awareness and Prevention:** GLOW shall provide employee training, on an ongoing and regular basis, concerning awareness and prevention of online threats affecting women, including cyberstalking and online harassment, as well as privacy issues related to reproduction and reproductive rights. The first training under this Judgment shall occur no later than one hundred eighty (180) days after the Effective Date and training shall be no less than once in a calendar year.

32. **Responsible Reporting Program:** GLOW shall implement and maintain a program that will allow the responsible reporting to GLOW of security vulnerabilities that are found in any mobile application or online service offered by GLOW. The program shall include, at a minimum, the guidelines for GLOW's responsible reporting program and a point of contact at GLOW to whom a security vulnerability can be reported.

33. The terms of Paragraphs 14-32 of this Judgment shall expire no later than three (3) years after the entry of this Judgment.

IV. ASSESSMENT AND REPORTING REQUIREMENTS TO THE ATTORNEY GENERAL

34. For two (2) years from the date on which the Information Security Program is implemented in accordance with Paragraph 14, GLOW shall complete an annual privacy risk assessment addressing GLOW's efforts to comply with applicable privacy laws governing GLOW's products or services.

a. The privacy risk assessment shall also (i) consider online risks that women face, or could face, including gender-based risks, as a result of privacy or security lapses while using GLOW mobile applications or online services; (ii) consider the impact of any such risks, and (iii) document GLOW's efforts to mitigate any such risks.

b. GLOW shall deliver a copy of the final report of each annual privacy risk assessment to the California Attorney General's Office. To the extent permitted by the laws of

1 the State of California, the California Attorney General's Office shall treat the report as exempt
2 from disclosure under the relevant public records laws.

3 c. GLOW shall provide a copy of the final report of each annual privacy risk
4 assessment to GLOW's Chief Executive Officer, and GLOW's Board of Directors.

5 35. For two (2) years from the date on which the Information Security Program is
6 implemented in accordance with Paragraph 14, GLOW shall complete an annual security
7 assessment of GLOW mobile applications or online services which (i) are designed to maintain
8 MEDICAL INFORMATION and/or (ii) collect, store, process, use, transmit, and/or maintain
9 PERSONAL INFORMATION, MEDICAL INFORMATION, or SENSITIVE PERSONAL
10 DATA.

11 a. The assessment shall set forth the administrative, technical, and physical
12 safeguards applied to such GLOW mobile applications and online services and assess, by
13 reference to industry best practices, whether the safeguards are appropriate to GLOW's size and
14 complexity, the nature and scope of GLOW's activities, and the sensitivity of the PERSONAL
15 INFORMATION, MEDICAL INFORMATION, or SENSITIVE PERSONAL DATA that
16 GLOW maintains.

17 b. GLOW shall provide a copy of the final report of each annual security
18 assessment to the California Attorney General's Office. To the extent permitted by the laws of
19 the State of California, the California Attorney General's Office shall treat the report as exempt
20 from disclosure under the relevant public records laws.

21 c. GLOW shall provide a copy of the final written report of each assessment
22 to GLOW's Chief Executive Officer and GLOW's Board of Directors.

23 36. To the extent permitted by the laws of the State of California, the California
24 Attorney General's Office shall treat all reports and other materials submitted by GLOW pursuant
25 to this Judgment and the information contained therein as exempt from disclosure under the
26 relevant public records laws and shall otherwise refrain from publicly disclosing such reports,
27 materials, and information.
28

1 **V. MONETARY PROVISIONS**

2 37. In accordance with Business and Professions Code section 17206 and pursuant to
3 the agreements reflected herein, GLOW shall pay the Attorney General the amount of \$250,000
4 over two years in eight (8) installments. Payment shall be made by wire transfer to the California
5 Attorney General's Office pursuant to instructions provided by the California Attorney General's
6 Office, with the first installment paid no later than thirty (30) days after the Effective Date and
7 each successive installment paid every three months after the previous installment was paid. Any
8 of GLOW's successors or the assigns of all or substantially all of the assets of GLOW's
9 businesses shall be obligated to pay any remaining amount such that the amount is paid in full.

10 38. The Attorney General shall use said payment for attorneys' fees and other costs of
11 investigation and litigation, to defray costs of the inquiry leading to this Judgment, and, pursuant
12 to Business and Professions Code section 17206, for the Attorney General's enforcement of
13 California's consumer protection laws.

14 39. Except as otherwise expressly provided herein, each party shall bear its own
15 attorney's fees and costs.

16 **VI. GENERAL PROVISIONS**

17 40. This Court retains jurisdiction of this matter for purposes of construction,
18 modification, and enforcement of this Judgment.

19 41. Nothing in this Judgment shall be construed as relieving DEFENDANTS of their
20 obligations to comply with all state and federal laws, regulations, or rules, or as granting
21 permission to engage in any acts or practices prohibited by such law, regulation, or rule.

22 42. DEFENDANTS shall use reasonable efforts to notify their officers, directors,
23 employees, and agents responsible for carrying out and effecting the terms of this Judgment of
24 this Judgment and the requirements therein.

25 43. Notices and reports under this Judgment shall be served by email and by next-
26 business-day delivery service (such as FedEx) as follows:

27 To the People or People's counsel:
28

1 Yen P. (TiTi) Nguyen
2 Consumer Protection Section—Privacy Unit
3 California Attorney General’s Office
4 455 Golden Gate Ave., Suite 11000
5 San Francisco, California 94102-7004
6 Email: TiTi.Nguyen@doj.ca.gov

7 To DEFENDANTS or DEFENDANTS’ counsel:

8 Matthew D. Brown
9 Cooley LLP
10 101 California St., 5th Floor
11 San Francisco, California 94111-5800
12 Email: BrownMD@cooley.com

13 and

14 John B. Duncan
15 JB Duncan PC
16 103 East Blithedale Ave., Suite 7
17 Mill Valley, CA 94941
18 Email: John@duncanpc.com

19 44. This Judgment shall take effect immediately upon entry thereof.

20 45. The clerk is directed to enter this Judgment forthwith.

21 ORDERED AND ADJUDGED at San Francisco, California, this ____ day of _____,
22 2020.

23 _____
24 Judge of the Superior Court
25
26
27
28