

NO. _____

IN THE MATTER OF

STATE OF TEXAS

AND

TRUE BEGINNINGS d/b/a TRUE.com

§
§
§
§
§
§

IN THE DISTRICT COURT OF

TRAVIS COUNTY, TEXAS

_____ JUDICIAL DISTRICT

ASSURANCE OF VOLUNTARY COMPLIANCE

TO THE HONORABLE JUDGE OF SAID COURT:

The State of Texas, acting by and through Attorney General Greg Abbott and the Consumer Protection Division of the Office of the Texas Attorney General (“State”), and True Beginnings d/b/a True.com (“True.com” or “Respondent”) have agreed to the submission and entry of this Assurance of Voluntary Compliance (“Assurance” or “AVC”) for the Court’s approval and filing in accordance with the requirements of the Texas Deceptive Trade Practices – Consumer Protection Act (“DTPA”), Tex. Bus. & Com. Code Ann. § 17.58 (Vernon 2011 and Supp. 2013).¹

DEFINITIONS

- I. For purposes of this AVC, the following definitions shall apply:
 - A. “Respondent” or “True” shall mean True Beginnings d/b/a TRUE.COM and its officers, agents, representatives, employees, successors and assigns and shall be binding upon the reorganized debtor and any subsequent successors or assigns.
 - B. “Online dating service provider” means a person or entity engaged in the business of offering or providing to its members access to dating or compatibility evaluations

¹ The DTPA authorizes the consumer protection division to accept an assurance of voluntary compliance with respect to any act or practice which violates the DTPA from any person who is engaging in, has engaged in, or is about to engage in the act or practice. The DTPA requires that an assurance must be in writing and filed with and subject to the approval of the district court in the county in which the alleged violator resides or does business or in the district court of Travis County. See, TEX. BUS. & COM. CODE §

between persons through the Internet to arrange or facilitate the social introduction of two or more persons for the purpose of promoting the meeting of individuals;

- C. “Member” means a person who submits Personal Information or Highly Personal Intimate Information to Respondent in order to utilize Respondent’s online dating service and includes persons who in addition to providing such information to Respondent, also pay Respondent for its services as an online dating service provider;
- D. “Criminal background check” is defined in Section 106.003 of the Internet Dating Safety Act, Tex. Bus. & Com. Code Ann. § 106.001, *et seq.*, and means that Respondent has initiated a name search for a person’s convictions for any: (a) felony offense; (b) offense the conviction or adjudication of which requires registration as a sex offender under Chapter 62, Texas Code of Criminal Procedure; and (c) offense for which an affirmative finding of family violence was made under Article 4.013, Texas Code of Criminal Procedure;
- E. “Personal information” or “PI” shall mean individually identifiable information from or about an individual consumer including, but not limited to: (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (d) a mobile or other telephone number; (e) a Social Security number; (f) a driver’s license number or any other government-issued identification number; (g) a bank account, debit card or credit card account number; (h) a persistent identifier, such as an Internet Protocol (IP) address, User ID, device ID or a customer number held in a “cookie;” and (i) photos and videos;

- F. “Highly personal intimate information” or “HPII” shall mean any information provided to Respondent by a consumer describing the consumer’s sexual preferences, habits, thoughts, experiences and searches for partners, which can be associated by Respondent with the consumer’s personal information.
- G. “Internet Dating Safety Act” shall mean Texas Internet Dating Safety Act, Tex. Bus. & Com. Code Ann. § 106.001, *et seq.*
- H. “Clear(ly) and conspicuous(ly)” shall mean:
1. In textual communications (e.g., printed publications or words displayed on the screen of a computer or mobile device), the required disclosures are of a type, size, and location sufficiently noticeable for an ordinary consumer to read and comprehend them, in print that contrasts highly with the background on which they appear;
 2. In communications disseminated orally or through audible means (e.g., radio or streaming audio), the required disclosures are delivered in a volume and cadence sufficient for an ordinary consumer to hear and comprehend them;
 3. In communications disseminated through video means (e.g., television or streaming video), the required disclosures are in writing in a form consistent with subpart (1) of this definition and shall appear on the screen for a duration sufficient for an ordinary consumer to read and comprehend them, and in the same language as the predominant language that is used in the communication;
 4. In communications made through interactive media, such as the Internet,

online services, and software, the required disclosures are unavoidable and presented in a form consistent with subpart (a) of this definition, in addition to any audio or video presentation of them; and

5. In all instances, the required disclosures are presented in an understandable language and syntax; in the same language as the predominant language that is used in the communication; and include nothing contrary to, inconsistent with, or in mitigation of any statement contained within the disclosure or within any document linked to or referenced therein.

I. “Appropriately labeled hyperlink” means that the hyperlink label is an accurate description of the landing page to which the hyperlink leads.

COMPLIANCE TERMS

II. Respondent hereby assures the State that it and its officers, agents, servants, employees, and attorneys, and any other person in active concert or participation with Respondent will comply with the terms set out in the following paragraphs A through M.

Internet Dating Safety Act

A. Respondent shall not represent in any manner, expressly or by implication, that it conducts criminal background checks, criminal background screenings, criminal screening or background checks (Criminal Screenings) of members unless such Criminal Screenings are in compliance with the requirements of the Internet Dating Safety Act, Section 106.003;

B. Within 30 days of entry of this Assurance, Respondent shall either

1. Cease to represent directly or indirectly that it conducts Criminal Screenings, delete from its website all representations that it conducts such screenings and post at its website clear and conspicuous notice as required by Section 106.004 of the Internet Dating Safety Act, disclosing that it does not conduct criminal background checks; OR
 2. Begin conducting criminal background checks which comport with the requirements for criminal background checks as defined in Section 106.003 of the Internet Dating Safety Act, and post at its website a notice and information required by Section 106.005(b) of the Internet Dating Safety Act, attached here as Exhibit 1 and incorporated for all purposes.
 3. An appropriately labeled hyperlink to the notices described in the preceding paragraphs (1) and (2) shall be presented on each page of Respondent's site which makes reference to online safety or to Criminal Screenings.
- C. Respondent shall not misrepresent the scope or type of any background screening or vetting of members which it may conduct. For example, Respondent shall not represent that it screens potential members for felony offense convictions unless such is in fact the case and they screen for all such convictions.

Accurate And Up- To- Date Privacy Policy

- D. Within 60 days of entry of this Assurance, Respondent shall develop and maintain an up-to-date and accurate privacy policy. The privacy policy shall be available at Respondent's web site and shall be linked to the home or landing page or screen of

the web site, and at each page or area of the site where any PI or HPPII is collected from consumers. On the landing page accessed after selecting the privacy link, Respondent shall provide its privacy policy which at a minimum must meet the following requirements:

1. Use direct, language understandable to the intended audience using a format and font that is reasonably easy to follow;
2. Disclose all material terms of Respondent's privacy policies and practices including the following:
 - a. Each and every category or type of PI and HPPII collected by True;
 - b. The internal use by True of each category of PI and HPPII;
 - c. The identity of each third party-whether affiliated or unaffiliated with True-with whom True shares the members PI and HPPII;
 - d. The length of time that True will maintain each category of PI and HPPII;
 - e. Whether True continues to maintain PI and HPPII which a member has deleted;
 - f. Whether True maintains a member's PI and/or HPPII after the member has terminated membership in True.
3. Include hyperlinks to any referenced third parties' privacy policies; and
4. Include an e-mail and physical address for Respondent that consumers can use to obtain further information regarding True's privacy practices.

- E. If Respondent's Privacy Policy provides that True may share the PI or HPPII of members with third parties without further notice to or consent from a member, Respondent will clearly disclose that fact to members and further, prior to sharing the PI or HPPII of members, Respondent will review the privacy policies and practices of those third parties to assure that, at a minimum, such third parties provide substantially the same privacy safeguards afforded under Respondent's policy and by contract, Respondent will prohibit third parties from further sharing, disclosing or transferring the PI or HPPII of members. The restrictions in this paragraph do not prohibit True from sharing, disclosing or transferring member information with service providers for the purpose of processing transactions.
- F. In the event that Respondent should be acquired or substantially all of its assets transferred, the PI and/or HPPII of its members shall not be shared or transferred without Respondent first obtaining the express, affirmative opt-in consent of the member.

Information Security And Privacy Program

- G. Within 90 days of entry of this Assurance, Respondent shall establish and implement, and thereafter maintain, a comprehensive information security and privacy program that is reasonably designed to protect the security, confidentiality, and integrity of all PI and HPPII collected from or about consumers by respondent or by any corporation, subsidiary, division, website, or other device or affiliate owned or controlled by Respondent. This section may be satisfied through the review and maintenance of an

existing program so long as that program fulfills the requirements set forth in this section.

H. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the personal information collected from or about consumers, including:

1. the designation of an employee or employees to coordinate and be accountable for the information security program;
2. the identification of material internal and external risks to the security, confidentiality, and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) information systems, including network and software design, information processing, storage, transmission, and disposal; (3) prevention, detection, and response to attacks, intrusions, or other systems failures;
3. the design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures;

4. the evaluation of Respondent's current information collection and retention practices;
 5. the development and use of reasonable steps to select and retain employees, contractors, agents and service providers capable of appropriately safeguarding personal information they receive from respondent, and requiring employees, contractors, agents, affiliates and service providers by contract to implement and maintain appropriate safeguards; and
 6. the evaluation and adjustment of the information security and privacy program in light of the results of the testing, evaluation and monitoring required by this section, any material changes to any operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its information security and privacy program.
- I. Such program must further
1. Assure that Respondent does not maintain, store, or transfer the payment card authentication data of Consumers in any form unless necessary for a documented business need;
 2. Assure that Respondent's practices are in compliance with the Restore Online Shopper's Confidence Act ("ROSCA"), 15 U.S.C. § 8401, *et seq.*; *see also* 28 U.S.C. § 959(b);
 3. Purge or arrange to purge payment card authentication data of members as soon as practicable once the business need expires for the maintenance or

storage of such and assure that such information is purged using a secure deletion tool;

4. Assure that Respondent does not maintain or store the PI or HPII of members unless necessary for a documented business need and that when such information is no longer needed it shall be purged using secure deletion tools.

Compliance Reporting

J. Respondent further assures the Attorney General that, in connection with its compliance with this Assurance, Respondent shall take the following action:

1. With respect to the Internet Dating Safety Act (“Act”) section of this Assurance, Respondent shall submit to the OAG a statement attested to by Respondent’s president or chief executive officer explaining the steps Respondent has taken to comply with such section and with the requirements of the Act. Such report shall be due [To be negotiated, suggested: 30 days] days after entry of this Assurance and thereafter, on November 1st of each year for five consecutive years.
2. With respect to the Privacy Policy section of this Assurance (paragraphs D through F), Respondent shall submit to the OAG a statement attested to by its privacy officer or chief executive officer explaining the steps Respondent has taken to comply with such section and shall include a copy of its privacy policy. Such report shall be due [To be negotiated, suggested: 45days] days after entry of this Assurance and thereafter, on November 1st of each year for five consecutive years.

3. With respect to of the Information Security and Privacy Program section of this Assurance (paragraphs G through I), Respondent shall obtain initial and biennial assessments and reports (“Assessments”) from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. Professionals qualified to prepare such assessments shall be: a person qualified as a Certified Information System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA); a person holding Global Information Assurance Certification (GIAC) from the SANS Institute.

a. The reporting period for the Assessments shall cover:

- (i) the first one hundred and eighty (180) days after entry of this Assurance for the initial Assessment, and
- (ii) each two (2) year period thereafter for ten (10) years after entry of of this Assurance for the biennial Assessments.

b. Each Assessment shall:

- (i) set forth the specific administrative, technical, and physical safeguards that Respondent has implemented and maintained during the reporting period;
- (ii) explain how such safeguards are appropriate to respondent’s size and complexity, the nature and scope of respondent’s activities, and the sensitivity of the personal information collected from or about consumers;

- (iii) certify how the safeguards that have been implemented meet or exceed the protections required by this Assurance;
 - (iv) certify that the security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of PI and HPPI is protected and has so operated throughout the reporting period;
and
 - (v) certify that Respondent's information collection practices are consistent with all representations made in its privacy policy.
- c. In addition, the initial assessment shall include an explanation of Respondent's data retention policies and practices prior to entry of this Assurance and changes made to those policies and practices post entry of this Assurance and shall specifically report on any action taken, or planned, to purge Respondent's files of the PI and HPPI and payment card authentication data of the 43 million persons who were True members as of the date of entry of this Assurance.
- d. If Respondent's data retention policies elect to retain the PI and HPPI of paying members whose most recent payment was made to Respondent more than 12 months prior to the date of an assessment, the assessment shall include a report of each type of information Respondent is retaining and Respondent's documented business need for retaining such information.

- e. Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies.

Notice To Officers, Directors, Employees And Agents

- K. Respondent shall deliver copies of this Assurance to
 - 1. all current and future principals, officers, directors, and managers;
 - 2. all current and future employees, agents, and representatives having responsibilities relating to the subject matter of this order, and
 - 3. any business entity resulting from any change in structure or reorganization of Respondent.
- L. Respondent shall deliver this Assurance to such current personnel within thirty (30) days after entry of this Assurance, and to such future personnel or business entity at least ten (10) days prior to the person or entity's assumption of such position or responsibilities.
- M. Respondent shall secure a signed and dated statement acknowledging receipt of this Assurance from all persons receiving a copy of this Assurance pursuant to this section and will provide such to the Attorney General, upon the Attorney General's request.

GENERAL PROVISIONS

- III. The following general provisions apply to this AVC:
 - A. The parties to this AVC expressly understand and agree that this AVC shall not be construed in any way as an admission on the part of the Respondent or any of its

corporate affiliates of any violation of the DTPA or of any other law or of any other conduct or of any liability whatsoever to any party, all of which is expressly and vigorously denied;

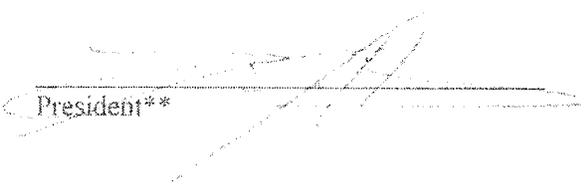
- B. Nothing in this AVC shall be construed as a waiver of any private rights, causes of action, or remedies of any person against the Respondent with respect to its practices described herein;
- C. Nothing in this AVC shall be viewed, interpreted, or understood as providing an exemption to the Respondent from any State or Federal law, rule, or regulation;
- D. This AVC shall be governed by § 17.58 of the DTPA, and shall remain in effect until rescinded by agreement of the parties or voided by a Court of competent jurisdiction for good cause and venue of this cause is proper in Travis County, Texas and the State District Court has exclusive jurisdiction for this Assurance;
- E. It is also understood by the Respondent that the subsequent failure to comply with the terms of the AVC is prima facie evidence of a violation of the Deceptive Trade Practices-Consumer Protection Act;
- F. The Office of the Attorney General has authority in this matter under Section 17.47 of the DTPA;
- G. This AVC states the entire agreement between the parties respecting the subject matter stated herein.
- H. It shall not be considered a violation of the AVC for TRUE to post information at the TRUE.com public website which members have provided to TRUE for that purpose.

- G. This AVC states the entire agreement between the parties respecting the subject matter stated herein.
- H. It shall not be considered a violation of the AVC for TRUE to post information at the TRUE.com public website which members have provided to TRUE for that purpose.

AGREED this 22nd day of November, 2013.

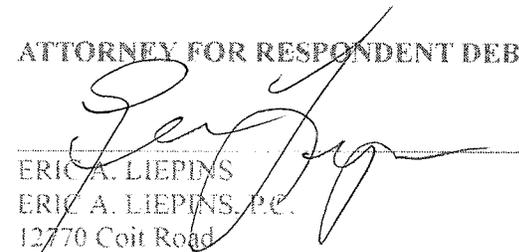
AGREED AS TO SUBSTANCE AND FORM AND ENTRY REQUESTED:

FOR TRUE BEGINNINGS D/B/A TRUE.COM:



President**

ATTORNEY FOR RESPONDENT DEBTOR:



ERIC A. LIEPINS
ERIC A. LIEPINS, P.C.
12770 Coit Road
Suite 1100
Dallas, Texas 75251
Phone
Fax

ATTORNEYS FOR THE STATE OF TEXAS

GREG ABBOTT
Attorney General of Texas

DANIEL T. HODGE
First Assistant Attorney General

JOHN B. SCOTT
Deputy Attorney General for Civil Litigation

TOMMY PRUD'HOMME
Chief, Consumer Protection Division

D. ESTHER CHAVEZ
State Bar No. 04162200
Assistant Attorneys General
Office of the Attorney General
Consumer Protection Division
P.O. Box 12548
Austin, Texas 78711
(512) 475-4628 Phone
(512) 463-1267 Fax
Esther.Chavez@texasattorneygeneral.gov