pillsbury

Pillsbury Winthrop Shaw Pittman LLP
2300 N Street, NW | Washington, DC 20037-1122 | tel 202.663.8000 | fax 202.663.8007

Lauren Lynch Flick
tel 202.663.8166
lauren.lynch.flick@pillsburylaw.com

June 27, 2013

Donald S. Clark. Secretary
Federal Trade Commission
Room H-113
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: **REQUEST FOR CONFIDENTIAL TREATMENT**

Dear Mr. Clark:

Pursuant to the Children's Online Privacy Protection Act Final Rule announced on December 19, 2012, and on behalf of Privacy Vaults Online, Inc. d/b/a PRIVO, a previously approved Commission Safe Harbor Program provider, I am submitting herewith PRIVO's complete Membership Agreement, including at Exhibit B its revised Privacy Assurance Program Guidelines, and its Self-Evaluation Form.

It is respectfully requested that the Membership Agreement itself, Exhibit F thereto, and the Self-Evaluation Form be kept confidential and not made part of the public record.

A redacted copy for public disclosure is also provided.

The Membership Agreement is a private agreement dealing primarily with compensation of the Safe Harbor, the use of the Safe Harbor's trademarks, and the Safe Harbor's business method. The Self-Evaluation Form reflects the Safe Harbor's proprietary business process and is essential to the Safe Harbor's business operations. Release of these documents to the public would substantially hinder the Safe Harbor's ability to offer its unique service and put it at a competitive disadvantage in an increasingly competitive market. The Safe Harbor considers these documents to be trade secrets and protectable from disclosure under FOIA.

Should the Commission require additional information, please do not hesitate to communicate with the undersigned.

Respectfully submitted,

/s/
Lauren Lynch Flick

Enclosure

PRIVO®
PRIVACY, PERMISSION & TRUST

Confidential and Proprietary

PRIVACY ASSURANCE PROGRAM
MEMBERSHIP AGREEMENT

REDACTED

EXHIBITS

EXHIBIT A

1. Online Service Name: : _____

   URL: _____

2. Online Service: _____

   URL:_____

3. Online Service: _____

   URL: _____

EXHIBIT B

Privacy Assurance Program Guidelines

Program Requirements for the Collection, Use, and Disclosure of Information from Children

Since August 2004, the Federal Trade Commission has authorized PRIVO to administer this Privacy Assurance Program (the "Safe Harbor") to provide protections for Children, through a self-regulatory mechanism, that are substantially the same as or greater than those provided by Sections 312.2 through 312.8 and 312.10 of the Commission's Children's Online Privacy Protection Rule (16 C.F.R. Part 312) ("Rule") implementing the Children's Online Privacy Protection Act, 15 U.S.C. § 6501 et seq. ("COPPA"), as amended.

The following principles are designed to assure that the participants in the Safe Harbor program ("Members") establish and maintain data Collection activities and privacy practices that comply with the Rule and additionally are consistent with industry best practices and capable of evolving as new technologies, capabilities and threats emerge. These Guidelines guide PRIVO in its determinations as to the fitness of proposed Members for inclusion (or retention) in the Safe Harbor and must be formally adopted and honored by Members as provided in the Membership Agreement. All capitalized terms used herein that are not otherwise defined have the meaning given to them in the Membership Agreement.

The Safe Harbor is available to the Operator of any Online Service of any nature, including websites, games, applications, features, plug ins, platforms, widgets or similar services and properties, regardless of whether the Online Service is Directed to Children, Directed to Children but Attracts a Mixed Audience, Not Directed to Children, Not Directed to Children but has Actual Knowledge that it is Collecting Personal Information from a site that is Directed to Children or from a Child, or Not Directed to Children but associated with Age-Restricted Goods and Services. As a baseline, Members must comply with the Rule which prohibits unfair or deceptive acts or practices in connection with the Collection, use, Release, and/or Disclosure of Personal Information from and about Children on the Internet. In addition, Members must implement each of the nine Requirements described below, unless it is noted that certain Requirements are not applicable to the Member's type of Online Service.

Members whose Online Services are deemed to be compliant with these Requirements must display the appropriate PRIVO Seal. Members whose Online Services are found to be non-compliant are subject to the enforcement and sanction procedures described in Requirement 9 hereof.

Requirement 1: Self-Evaluation; Privacy by Design Principles

On an on-going basis, each Member must analyze, including through the use of PRIVO self-assessment collateral and cooperation with PRIVO's independent analyses of, the functionality of its Online Service and its practices with respect to the Collection, Disclosure, Release, use and safeguarding of information regarding Children under 13 years of age (or of all minors at the option of the Member), including any business objectives that underlie those practices. The goals of such analysis include (i) assessing the extent to which Children comprise the audience of the Online Service; (ii) assessing the extent to which the Online Service Collects, uses, Releases, or Discloses Personal Information of Children; (iii) assessing the extent to which Third Parties Collect, use, Release, or Disclose Personal Information of Children through the Online Service; (iv) assessing the appropriateness of any age-screening mechanisms; (v) assessing the appropriateness of any Parental verification methods and notices employed by Member, or applicability of any exception to stated Parental verification methods to Member's Online Service; (vi) assuring that the Member does not Collect, use, Disclose or Release more information than is reasonably necessary to conduct its online activities; (vii) assuring that Member and any Third Party Operators associated with Member's Online Service adequately safeguard information Collected, including Deleting Personal Information when it is no longer reasonably necessary to fulfill the purposes for which it was Collected and to take precautions against Disclosure or Release of such information when Deleting it; and (viii) assuring that the Member's practices are otherwise in conformity with prevailing generally-accepted privacy principles. Members must incorporate privacy protections into the initial design of their Online Services, and each revision, add-on or additional feature added to the Online Service thereafter. Finally, through on-going self-assessment, Members are expected to partner with PRIVO in identifying new or evolving marketing or information

practices in the online industry to determine whether they present equivalent risks to those which currently require the giving of notice or securing of Parental consent, as well as evolving methods of Parental verification that have the promise of providing protections equivalent to those enumerated herein.

Requirement 2: Appropriate Use of Age-Screening, Blocking

A Member whose Online Service is deemed to be Directed to Children, based on the assessment undertaken in Requirement 1, shall comply with Requirements 1 through 9 hereof. (312.3)

A Member whose Online Service is deemed to be Directed to Children but Attracts a Mixed Audience may implement a Neutral Age-Screen prior to Collecting any Personal Information. Such an Online Service must comply with Requirements 1 through 9 hereof with respect to those Users who self-identify as being Children. In addition, such Members must ensure that, although a self-identified Parent establishes an account for a Child, the Member receives appropriate consent under Requirement 5 for Collecting, using or Disclosing any Personal Information associated with the Child account. Finally, such Members must not use the Neutral Age-Screen to block Children from participation in the Online Service. (312.2)

A Member whose Online Service is deemed to be Not Directed to Children must comply with Requirements 1, 2 and 3 hereof only, except that, if the Member receives Actual Knowledge that it is Collecting Personal Information from a Child, it must comply with Requirements 1 through 9 with respect to that Child, or may implement procedures to block that Child from interacting further with the Online Service or those portions of it that involve the Collection, Use or Disclosure of Personal Information. (312.3).

A Member whose Online Service deals with Age-Restricted Goods and Services must comply with Requirements 1, 2 and 3 hereof and additionally must display the PrivoBlock™ seal, except that, if the Member receives Actual Knowledge that it is Collecting Personal Information from a Child, it must implement procedures to block that Child from interacting further with the Online Service.

Requirement 3: Online Disclosure of Information Privacy Practices

Members must post a prominent Link that is clearly labeled *Privacy Policy* or such similar notice that Links the User to a description of the Member's information Collection, use, and Disclosure practices. (312.3(a), 312.4(d)). In the case of an Operator of an Online Service other than an Online Service Directed to Children, the Link must Link the User to the portion of the Privacy Policy that addresses the Member's information practices specific to Children. In addition, Members must post their Privacy Policy or provide a Link to it in any application store or similar platform that offers the capability of doing so.

The Privacy Policy Link must be plainly visible on the homepage, or landing page in the case of an application, and, for an Online Service that is Directed to Children, at each location where Personal Information is Collected from Children and in close proximity to the requests for information in each such area. If only a portion of an Online Service is Directed to Children, the Privacy Policy Link must be plainly visible on the first page of the Children's section of the Online Service, and Link the User to the portion of the Privacy Policy specific to Children.

Privacy Policies must be clear and understandable, and should not contain unrelated, contradictory, or confusing material. Privacy Policies must describe the following information:

A. Member Contact Information: Members must include their complete contact information, as well as that of any other Operators that Collect or maintain Personal Information from Children through the Online Service. Such information must include the Operator's name, mailing address, telephone number, and email address. In cases where more than one company is deemed to be an Operator of the Online Service Directed to Children, the Member may choose to respond to all inquiries from Parents concerning each of the identified Operators' privacy policies. In such case, the Member's Privacy Policy need only list the names of all persons or companies Collecting Personal Information through the Online Service.

B. Types of Personal Information Collected: Members must describe the types of Personal Information Collected and state whether the Online Service enables the Child to make Personal Information publicly available.

C. Use of Personal Information: Members must describe how Personal Information is used.

D. Disclosure of Personal Information: Members must state whether Personal Information is Disclosed to Third Parties.

E. Access to Information: Members whose Online Services are Directed to Children must state that Parents can review the Child's Personal Information, have such information Deleted, and refuse to permit further Collection or use of the Child's Personal Information. Members must also indicate the procedures that the Parent must follow to access their Child's Personal Information.

Requirement 4: Direct Notice to Parents

Members whose Online Services are Directed to Children must make reasonable efforts in light of available technology to ensure that a Parent of a Child receives notice of the Member's information Collection, use, and Disclosure practices with regard to Children, including notice of any material change in the Collection, use, or Disclosure practices to which the Parent had previously consented. (312.4) Except for certain circumstances described under Requirement 5D below, Members must meet the requirements described above and obtain prior verifiable parental consent before they are allowed to Collect Personal Information from Children.

Direct Notices to Parents must be clear and understandable, and should not contain unrelated, contradictory, or confusing material. The contents of the Direct Notice to Parents will vary depending on the context which requires the giving of the Direct Notice.

A. Where Member Must Obtain Parent's Affirmative Consent to the Collection, Use or Disclosure of a Child's Personal Information: (i) the Member must state that it has Collected the Parent's Online Contact Information from the Child (and the Child or Parent's name if it has Collected that information) for the purposes of obtaining the Parent's consent under COPPA; (ii) the Member must state that the Parent's consent is required for the Collection, use, or Disclosure of Personal Information from the Child, and that Member will not do so if the Parent does not give consent; (iii) the Member must state what additional items of information it intends to Collect from the Child, as well as potential opportunities for the Disclosure of Personal Information if the Parent gives its consent; (iv) the Member must provide a Link to its Privacy Policy; (v) the Member must provide the method(s) by which a Parent may give such consent; (vi) the Member must state that it will Delete the Parent's Online Contact Information if the Parent does not provide the consent in a reasonable period of time. (312.4(c)(1))

B. Voluntary Notice to Notify Parent of a Child's Participation In An Online Service That Does Not Collect, Use or Disclose Children's Personal Information: (i) the Member must state that the Member has Collected the Parent's Online Contact Information from the Child to provide notice and subsequent updates to the Parent of the Child's participation in the Online Service, which does not otherwise Collect, use or Disclose Personal Information; (ii) the Member must state that the Parent's Online Contact Information will not be used or Disclosed for any other purpose; (iii) the Member must state that the Parent may refuse to permit the Child's participation and require Deletion of the Parent's Online Contact Information and how to do so; (iv) the Member must provide a Link to Member's Privacy Policy. (312.4(c)(2))

C. Where Member Intends to Communicate With the Child Multiple Times: (i) the Member must state that it has Collected the Child's Online Contact Information from the Child to provide multiple online communications to the Child; (ii) the Member must state that it has Collected the Parent's Online Contact Information from the Child to notify the Parent that the Child has registered to receive multiple online communications from the Member; (iii) the Member must state that the Online Contact Information Collected from the Child will not be used for any other purpose, Disclosed or combined with any other information Collected from the Child; (iv) the Member must state that the

Parent may refuse to permit further contact with the Child and require Deletion of the Parent's and Child's Online Contact Information, and how to do so; (v) the Member must state that if the Parent does not respond to the Direct Notice to Parent, the Member may use the Child's Online Contact Information for the purpose stated in the Direct Notice to Parent; (iv) the Member must provide a Link to its Privacy Policy. (312.4(c)(3))

D. Where Member Has Collected Personal Information to Protect a Child's Safety: (i) the Member must state that the Member has Collected the name and Online Contact Information of the Child and the Parent to protect the safety of a Child; (ii) the Member must state that the information will not be used or Disclosed for any other purpose; (iii) the Member must state that the Parent may refuse to permit the use and require Deletion of the information and how to do so; (iv) that if the Parent fails to respond to the Direct Notice to Parent, the Member may use the information for the purpose stated in the Direct Notice to Parent; (v) the Member must provide a Link to Member's Privacy Policy. (312.4(c)(4))

Requirement 5: Prior Verifiable Parental Consent

A. Generally: Members must obtain verifiable Parental consent before any Collection, use, or Disclosure of Personal Information from Children. Members must also obtain such consent to any material change in the Collection, use, or Disclosure practices to which the Parent has previously consented. (312.5(a))

B. Method for Obtaining Verifiable Parental Consent: To comply with Requirement 5, Members must obtain prior verifiable Parental consent by a method that is reasonably calculated, in light of the available technology, to ensure that the person providing consent is the Child's Parent. (312.5(b))

Methods to obtain prior verifiable Parental consent include: (i) providing a consent form to be signed by the Parent and returned to the Member by postal mail, facsimile or electronic scan; (ii) requiring the Parent to use a credit card, debit card or other online payment system that provides notice of each discrete transaction to the primary account holder in connection with a monetary transaction; (iii) having a Parent call a toll-free telephone number staffed by trained personnel or connect to such personnel via video-conference; (iv) verifying the Parent's identity by checking a form of government issued identification against databases of such information, provided that Member Deletes the Parent's information promptly after the verification is made; (v) using the PrivoLock™ System; or (vi) any other method deemed to be at least as reliable as the methods enumerated herein.

Members must give the Parent the option to consent to the Collection and use of the Child's Personal Information without consenting to Disclosure of that information to Third Parties.

C. Circumstances in Which An "Email" Coupled with Additional Verification Steps Provide Adequate Assurance that the Person Giving Consent is the Child's Parent: Members that do not Disclose Children's Personal Information may secure Parental consent by contacting the Parent via the Parent's Online Contact Information Collected from the Child, coupled with additional steps to provide assurances that the person providing consent is the Child's Parent. Additional steps may include: (i) sending a confirmatory email after receipt of Parent's consent in response to the original email; (ii) obtaining a postal address or telephone number from the Parent and confirming the Parent's consent after its receipt through a letter or telephone call using the information Collected from the Parent; (iii) using the PrivoLock™ System. Members using this method must also provide notice to the Parent that the Parent can revoke its consent given in response to the original email. Members are expected to partner with PRIVO in analyzing the availability and reliability of other "additional steps" that develop over time in response to technological or other developments and implement additional steps in consultation with PRIVO that appear to offer protections beyond those identified herein. (312.5(b)(2)(vi))

D. Exceptions to Verifiable Parental Consent: Even though verifiable Parental consent is required under most situations before a Member is permitted to Collect, use, or Disclose a Child's Personal Information, there are situations in which a Member will be allowed to Collect some Personal

Information before obtaining consent from the Child's Parent. The exceptions to prior verifiable Parental consent are as follows:

- *Required Parental Consent* - Members may Collect the first name or Online Contact Information of a Child or Parent to be used for the sole purpose of obtaining the required Parental consent. If a Member has not obtained Parental consent after a reasonable time from the date of the information Collection, the Member must Delete such information from its records. Members that Collect name or Online Contact Information from a Child under this exception must provide the Direct Notice to Parent described in Requirement 3. (312.4(c)(1))

- *Voluntary Notice and Updates to Parent Regarding Child's Participation in an Online Service that Does Not Otherwise Collect, Use, or Disclose Personal Information* - Members may Collect a Parent's Online Contact Information to provide the voluntary Direct Notice to Parent described in Requirement 3. Members may not use or Disclose the information for any other purpose. (312.4(c)(2))

- *One-Time Request* - Members may Collect a Child's Online Contact Information from the Child for the sole purpose of responding directly, on a one-time basis, to a specific request from the Child. Members that Collect the Child's Online Contact Information from a Child under this exception must not use the information to re-contact the Child after the initial response and must Delete the Child's Personal Information. Direct notice is not required under this exception. (312.4(c)(3))

- *Multiple Requests* - Members may Collect a Child's Online Contact Information from a Child to be used to respond directly more than once to a specific request from the Child so long as the information is not used for any other purpose, Disclosed, or combined with any other information Collected from the Child. Members that obtain the Child's Online Contact Information from a Child under this exception must also collect the Online Contact Information of the Child's Parent and provide the Direct Notice to Parent in Requirement 3. (312.4(c)(3))

- *Child Safety* - Members may Collect the Child's and Parent's first name and Online Contact Information to protect the safety of a Child, provided such information is not used or Disclosed for any other purpose. Members that obtain the Online Contact Information from a Child under this exception must provide the Direct Notice to Parent in Requirement 3. (312.4(c)(4))

- *Additional Safety Concerns* - Members may Collect a Child's first name or Online Contact Information to protect the security or integrity of its Online Service, to take precautions against liability, to respond to judicial process, or to provide information to law enforcement agencies or investigations on matters related to public safety so long as the information is not used for any other purpose. Direct Notice to Parent is not required under this exception. (312.4(c))

- *Collection Limited to Persistent Identifier* - Members may Collect a Persistent Identifier and no other Personal Information in two situations: (i) the identifier is used solely for Support of Internal Operations; or (ii) the Member's Online Service is not itself Directed to Children but has Actual Knowledge that it is Collecting information from Users of another Online Service that is Directed to Children, the User whose Persistent Identifier is Collected affirmatively interacts with the Member, and the User's previous registration with the Member indicates that the User is not a Child. Members relying upon this exception must specifically address their practices with regard to the Collection of Persistent Identifiers in their assessment under Requirement 1. (312.5(c)(7), (312.5(c)(8))

  Activities that are currently identified as providing Support for Internal Operations are: (i) maintaining or analyzing the functioning of the Online Service, (ii) performing network communications; (iii) authenticating Users of, or personalizing the content on, the Online Service; (iv) serving contextual advertising or capping the frequency of advertising; (v) protecting the security or integrity of the User or Online Service; ensuring legal or regulatory compliance; and (vi) fulfilling a request by the Child under the One-Time Request and Multiple Request Exceptions in Requirement 5D above. (312.2)

Requirement 6: Access and Review

Members must provide Parents with the ability to access and review their Child's Personal Information. Parental review and access must consist of: (a) a description of the types or categories of Personal Information Collected from the Child by the Member and by other Operators on Member's Online Service; (b) the opportunity at any time to refuse to permit further use or Collection of Personal Information from the Child by the Member and to direct that the Personal Information Collected by the Member be deleted; (c) a means of reviewing any Personal Information Collected by the Member; and (d) a means of contacting any other Operator that Collected Personal Information from a Child through Member's Online Service in order to direct such Operator to provide access to, refuse further use or Collection of, or delete the Child's Collected Personal Information. (312.6)

In providing the ability for a Parent to access and review their Child's Personal Information, Members must take reasonable steps to ensure that the individual requesting access is the Child's Parent and to ensure that the process is not unduly burdensome for Parents. Acceptable steps for authenticating the identity of the individual online include a username and password unique to the individual or, if access is requested over the telephone, asking a series of questions that only a Parent of the Child would have knowledge of (e.g., Parent's name, mailing address, email address, Child's name, Child's email address, etc.)

Requirement 7: Restrictions on Information Collection

Members are prohibited from conditioning a Child's participation in an activity on the Child's Disclosing more Personal Information than is reasonably necessary to participate in such activity. (312.7)

Requirement 8: Confidentiality, Security and Integrity of Information

Members must establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of Personal Information collected from Children, including (i) implementing internal security measures that protect the confidentiality of the Child's Personal Information and protect such information from loss, misuse, unauthorized access, or improper disclosure, and (ii) only Releasing a Child's Personal Information to Third Parties who have given reasonable assurances of their ability to similarly protect such information from loss, misuse, unauthorized access, or improper disclosure. These practices must be included in the Member's self-evaluation pursuant to Requirements 1 and 9, and must address the required data protection practices of any Third Parties with which the Member contracts. If requested by PRIVO, Members must make appropriate IT personnel available for interview and permit on-site inspection of Member's practices. Members must not retain information longer than reasonably necessary. (312.8)

Requirement 9: Compliance/Enforcement

A. Program Representative: Members must appoint a program representative for the Online Service. The program representative shall be the individual responsible for overseeing the Online Service's compliance with the Privacy Assurance Program. The program representative shall be given the authority to investigate all inquiries concerning the Online Service's Privacy Policy and information practices and in a timely manner.

B. Initial, Quarterly and Annual Audits: As set forth in Requirement 1, Members must conduct an evaluation of their Online Service's information Collection, use, and Disclosure practices. Each Member will be required to complete and attest to the accuracy of the statements they make on a proprietary PRIVO self-evaluation form about their information practices. Once PRIVO receives the self-evaluation form, a PRIVO representative will independently review the Online Service's posted privacy policy, information practices, and the self-evaluation form for compliance with the Program Requirements. PRIVO will issue an Observations and Findings Report, review it with the proposed Member, and identify any modifications necessary to bring the Online Service into compliance with the Rule and Program Requirements. Once the Member's Online Service is determined to be in full compliance with the Program Requirements, it will then be listed as a Member participating in the Privacy Assurance Program. Members are required to complete a certification form quarterly identifying any additional features or changes in practices that have occurred since the Online Service was last certified/audited by PRIVO. Members are also required to complete a comprehensive self-

evaluation form on an annual basis to ensure that their Online Service's information practices are consistent with their posted privacy policies and the Program Requirements. Outside of these mandated review processes, Members are encouraged to contact PRIVO whenever making revisions to their operations or adding features to their Online Service as part of their on-going self-assessment required under Requirement 1.

C. Compliance Monitoring: Members must submit to monitoring of their Online Service's information practices. The purpose of monitoring reviews is to ensure that a Member's Privacy Policy is consistent with its Online Service's information practices, the Program Requirements, and evolving best practices in the industry. The compliance monitoring will be conducted at least annually, or more frequently in response to any changes identified on the Member's quarterly certification form. In addition, Members must also submit to periodic, unannounced reviews of their Online Service. These unannounced reviews will be used to further verify that the Member remains in full compliance with the Program Requirements.

If PRIVO determines that a violation of the Requirements has occurred, the Member is informed of such violation and the corrective actions that must be taken to bring the Member's Online Service into compliance. Failure to take the corrective actions can result in a number of consequences including removal from the Privacy Assurance Program and referral to the appropriate governmental agency.

D. Consumer Complaints/Monitoring: Members must provide the Parent and the Child with reasonable and effective means to submit complaints that they may have about the Member's information practices. The Privacy Assurance Program also offers the Parent and the Child with the opportunity to submit complaints about any Member directly to PRIVO. A PRIVO representative responds to all complaints immediately. Members must agree to work with PRIVO representatives in their efforts to resolve all complaints that are submitted to the Privacy Assurance Program.

Members must maintain records for a period of three (3) years of all complaints, concerns, or inquiries received about its Online Service and any responses to the consumer addressing such complaint or concern.

E. Membership Agreement: Members must execute the Privacy Assurance Program Membership Agreement. As part of this Agreement, Members agree to comply with the Program Requirements at all times. In the event that a Member fails to meet any of its obligations under the Membership Agreement, such actions would constitute a material breach of the Agreement and its membership in the Privacy Assurance Program would be terminated, if not cured as provided in the Membership Agreement.

F. Investigations/Referral to Governmental Agencies: If PRIVO determines, after a thorough investigation into the Member's information practices, that a Member is materially violating its posted Privacy Policy or any of the Requirements described above without remedy following a period of notice and opportunity to cure, PRIVO will refer such Member to the Federal Trade Commission for possible unfair and deceptive trade practices.

GLOSSARY

1.1 "Actual Knowledge" means that knowledge that an Online Service that is Not Directed to Children receives when (a) a child-directed content provider advises the Online Service of the content provider's child-directed nature, or when a representative of the general audience Online Service recognizes the child-directed nature of the content provider's Online Service; or (b) a Child, Parent, legal guardian or advocate on their behalf provides direct evidence of the Child's age such as its date of birth, age, grade in school to the Operator.

1.2 "Age-restricted Goods and Services" means products or services that are generally not considered appropriate for Children such as tobacco, alcohol, financial, gambling, adult/mature-themed products or services.

1.3 "Child" or "Children" means User(s) who are 12 years of age or younger.

1.4 "Collect" or "Collection" means gathering Personal Information from a Child in any way, including (a) requesting, prompting or encouraging Personal Information be submitted online; (b) allowing a Child to make Personal Information publicly available in an identifiable form IF the Operator does not take reasonable steps to delete all or virtually all Personal Information from a posting and its records before posting; (c) passive online tracking.

1.5 "Delete" means to remove Personal Information in a manner that it is no longer retrievable in the normal course of business.

1.6 "Directed to Children" means an Online Service or a portion thereof that (a) is targeted to Children (based on its subject matter, visual content, use of animated characters or child-oriented activities and incentives, music or other audio content, age of models, presence of child celebrities or celebrities who appeal to Children, language or other characteristics of the Online Service, as well as whether advertising promoting or appearing on the Online Service is directed to Children, or competent and reliable empirical evidence of audience composition and intended audience composition) and Children are its primary intended audience; or (b) has Actual Knowledge that it is Collecting Personal Information from a Child.

1.7 "Directed to Children but Attracts a Mixed Audience" means an Online Service that is otherwise Directed to Children but (i) Children are NOT its primary intended audience, (ii) the Online Service does not Collect Personal Information before employing a Neutral Age-Screen, and (iii) the Online Service complies with Requirements 4 and 5 of these Guidelines with respect to any self-identified Child.

1.8 "Direct Notice" means the information provided under Requirement 4 to a Parent regarding the practices of an Online Service with respect to Collecting, Disclosing, Releasing, and safeguarding the Personal Information of a Child, but does not include the Privacy Policy as posted to the Online Service or any application store.

1.9 "Disclose" or "Disclosure" means to Release Personal Information Collected from a Child in identifiable form for any purpose other than Support of Internal Operations, or make Personal Information Collected from a Child publicly-available in identifiable form by any means.

1.10 "Effective Date" has the meaning set forth in the preamble to the Membership Agreement.

1.11 "Internet" means the interconnected world-wide network of networks.

1.12 "Guidelines" means the Privacy Assurance Program Guidelines or set of principles designed to assure that Members establish and maintain data Collection activities and privacy practices that comply with the Rule and which guide Privo in determining the fitness of proposed Members for inclusion (or retention) in the Program.

1.13 "Link" means a hypertext link or an icon on a page on an Online Service, that a User can select and activate from a computer or other device by mechanical means such as a mouse, other pointing device, or

key, and whose activation automatically causes the Online Service's system to give the User access to another page on the Online Service or to another Online Service, without additional steps or additional input from the User.

1.14 "Mark" has the meaning set forth in the preamble to the Membership Agreement.

1.15 "Member" has the meaning set forth in the preamble to the Membership Agreement.

1.16 "Neutral Age Screen" means a method of requesting age information that permits Children to accurately provide their age and does not encourage Children to falsify their age. An example of a Neutral Age Screen is asking the Child to enter their date of birth without any restriction, including allowing them to enter any year of birth beginning with the current year.

1.17 "Not Directed to Children" means an Online Service that is not targeted to Children.

1.18 "Online Contact Information" means an identifier that permits online contact with a person, such as an email address, user ID for a service that permits direct contact such as VOIP, IM or video chat services.

1.19 "Online Service" means a service that is available over the Internet or that connects to the Internet or a wide-area network, including a webpage or website, virtual world, social networking service, desktop software application, mobile or other application, Internet-enabled gaming platform, voice-over-IP service, Internet-enabled location based service, plug in, ad network, analytics service, platform, widget or other service that allows for playing network-connected games, engaging in social media activities, purchasing goods and services online, receiving behaviorally targeted advertising, or interacting with other content.

1.20 "Operator" means (a) any person or entity that maintains an Online Service (other than an Online Service that operates solely on an intrastate basis) that is operated for commercial purposes and that Collects or maintains Personal Information from or about Users of that Online Service; (b) the person or entity for which Personal Information is collected or who offers products or services for sale through the Online Service; or (c) any Third Party Online Service that has Actual Knowledge that it is collecting Personal Information from an Online Service Directed to Children.

1.21 "Parent" means a biological, foster, adoptive or other legal guardian of a Child; and/or a school or educational institution that has been granted the authority to act on behalf of any of the aforementioned for the purpose of providing such consent as is needed for the Child's use of the Member's Online Service; and/or any other adult to whom any of the aforementioned has delegated the duty to manage the consent process relating to the Child generally.

1.22 "Persistent Identifier" means a code that can be used to recognize a User or device over time and across different Online Services. Examples include a cookie, IP address, processor or device serial number, or unique device identifier.

1.23 "Personal Information" means information that is Collected online and identifies an individual User or device, including (a) first AND last name; (b) home or other physical address including street name and name of city or a postal code that on its own provides a similar level of information; (c) Online Contact Information; (d) other screen or User name if it functions like Online Contact Information; (e) telephone number; (f) Social Security Number; (g) Persistent Identifier; (h) photograph, audio or video file that contains the image or voice of a Child; (i) geolocation information sufficient to identify name of street and city or town; (j) any other information Collected online from the Child about the Child or Parent and is combined with Personal Information listed in this definition.

1.24 "Privacy Policy" means a privacy policy or statement that informs Users about Member's online information practices, including its information practices with regard to Children, as appropriate, and that is to be implemented and published by the Member as provided for in the Program Requirements.

1.25 "Privo" has the meaning set forth in the preamble to the Membership Agreement.

1.26 "Program" has the meaning set forth in the preamble to the Membership Agreement.

1.27 "Program Requirements" has the meaning set forth in the preamble to the Membership Agreement.

1.28 "Release" means to share, sell, rent, or transfer Personal Information to any Third Party.

1.29 "Support for Internal Operations" means activities necessary to facilitate functioning of the Online Service but do not involve using or Disclosing information to contact a specific individual including through behavioral advertising, amass a profile on a specific individual or any other purpose. Such activities include: (a) maintaining/analyzing functioning of the Online Service; (b) performing network communications; (c) authenticating Users; (d) personalizing content to Users; (e) serving contextual advertising; (f) frequency capping; (g) protecting security/integrity of Online Service; (h) ensuring legal compliance; (i) fulfilling a one-time request from the Child, or to contact the Child multiple times, when prior Verifiable Parental Consent is not required under Requirement 5D.

1.30 "Third Party" means any person or entity that is not an Operator, or who provides Support for Internal Operations and does not Use or Disclose Personal Information for any other purpose.

1.31 "User" means a Child, the Parent of a Child, or legal guardian of a Child who accesses the Online Service.

EXHIBIT C

PRIVO® Privacy Assurance Program (PPAP) Certification Seal Logic

The PRIVO® Privacy Assurance Program (PPAP) *(Membership Agreement section 2.4(a))* requires Members to place the PRIVO Seal and associated text on the Member's homepage, the mobile app landing page, within the mobile app store if available, on any point within the site or app that prompts for data collection or sharing, and within the PPAP paragraph within the Member's Privacy Policy. The Member must choose one Seal from each of the two rows shown below. NOTE: The seals do not have to correspond to each other, except for the PRIVO APProved Seal. The Click to Verify Seals are intended to take the consumer from the Member's Privacy Policy to the PRIVO hosted certification page.

The logos will be delivered in EPS format with transparent backgrounds so that the Member can incorporate them into the site and/or app regardless of the background color of the individual pages. *(If you would like another format please let us know by sending an email to support@PRIVO.com with "Logo Request" in the subject line).*

The first row of images is the privacy certified seal choices. Members should display one of these images on the home page and on every page leading to kids' involvement *(e.g., join pages or other pages where information is collected).* In the case of mobile apps using the PRIVO APProved Seal, the placement should be in the landing page and at any point within the app that prompts for data collection or sharing. **This image must link to the Member's privacy policy**. Minimum Size Restriction: 95 x 40 px

The second row of images is the "Click to Verify" certification seal choices. Members should display one of these images in the Privacy Policy located within or adjacent to the paragraph describing the Member's safe harbor participation *(see paragraph below).* The Mobile APProved Seal, is an automatic "Click to Verify" seal. **When the user clicks on one of these seals, they must be directed to a certification URL provided to Member by PRIVO.** Minimum Size Restriction: 132 x 56 px

The following Header and Paragraph must be included in Member's Privacy Policy:

PRIVO®'s Privacy Assurance Program

[COMPANY NAME] is a licensee of the PRIVO® Privacy Assurance Program ("the Program"). [INSERT RIGHT-ALIGNED <IMG> TAG HERE] As a participating member in the Program, [COMPANY NAME] adheres to the strict information collection, use and disclosure requirements. PRIVO is an independent, third-party organization committed to safeguarding children's personal information collected online. PRIVO aims to help parents and their children exercise control over personal information while exploring the Internet. The certification seal posted on this page indicates that [COMPANY] has established COPPA compliant privacy practices and has agreed to submit to PRIVO's oversight and consumer dispute resolution process. If you have questions or concerns about our privacy practices, please contact us at [COMPANY'S PHONE NUMBER] or privacy@[COMPANY NAME].com. If you have further concerns after you have contacted us, you can contact PRIVO directly at privacy@privo.com.

EXHIBIT D

PROGRAM REPRESENTATIVE:

Designated Program Representative:

Program Representative's Telephone Number:

Program Representative's Email Address:

Program Representative's Mailing Address:

EXHIBIT E

COMPLIANCE COORDINATOR:

Designated Compliance Coordinator:

Compliance Coordinator's Telephone Number:

Compliance Coordinator's Email Address:

Compliance Coordinator's Mailing Address:

REDACTED