March 3, 2004

Secretary of the Commission
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580

RE: Request for Safe Harbor Approval by the Federal Trade Commission for Privo, Inc.'s Privacy Assurance Program Requirements under Section 312.10 of the Children's Online Privacy Protection Rule.

Dear Secretary:

Pursuant to the Children's Online Privacy Protection Rule ("Final Rule") announced in the Federal Register on November 3, 1999 (16 C.F.R. Part 312), Privo, Inc. ("Privo") respectfully submits the following application for approval as a safe harbor children's privacy program within the meaning of the Final Rule Section 312.10 implementing the Children's Online Privacy Protection Act (15 U.S.C. 6501 *et. seq.*). In addition to this original, Privo submits five (5) copies of this application for safe harbor approval, along with a 3 1/2" floppy disk containing the application in Microsoft Word format.

Privo's safe harbor application is divided into three parts:

Part I includes (i) a brief description of Privo and its Privacy Assurance Program and (ii) the full text of the Privacy Assurance Program Requirements ("Program Requirements")for which approval is sought by the Federal Trade Commission ("Commission");

Part II includes a comparison of each provision of Section 312.3 through Section 312.8 with the corresponding provisions of the Program Requirements; and,

Part III includes a statement explaining (i) how the Program Requirements and its applicable assessment mechanisms meet the requirements of the Final Rule, (ii) how the assessment mechanisms and compliance incentives required under Section 312.10(b)(2) and (3) provide effective enforcement of the requirements of the Final Rule.

6320 Augusta Dr. Suite 1101
P.O. Box 5535
Springfield, VA 22150
Phone: (703) 703.273.8100 Fax: (703) 783-8752
Website: http://www.privo.com

Privo wishes to thank the Commission in advance for its consideration. We look forward to working with the Commission during the review and approval process.

Respectfully submitted,

Albert Strong
Director, Privacy Assurance Program
Privo, Inc.

PART I: BACKGROUND INFORMATION ON PRIVO AND A COPY OF THE FULL TEXT OF THE PRIVACY ASSURANCE PROGRAM REQUIREMENTS

I(A) PRIVO AND THE PRIVACY ASSURANCE PROGRAM

Introduction

The Privacy Assurance Program is an independent compliance and enforcement program that assists companies in protecting information obtained from children online. Our program helps companies safeguard the rights of children by providing guidelines that companies can follow to ensure that the information they obtain from children is done in an open, secure, and reliable manner. From our Program Requirements for the collection, use, and disclosure of personal information from children to our PrivoLock™ System, our proprietary verifiable parental consent mechanism, we offer companies an integrated privacy program that is dedicated to the protection of personal information from children online.

Background

Privo was established in 2001 in response to the increased need for an effective and meaningful technological solution that enables companies to create rewarding relationships with children online while meeting the expectations and concerns of parents and governmental regulators.

As its primary mission at the time of its creation as an infomediary service, which allows companies that wish to collect personal information from children online to do so in an efficient and compliant way, Privo began to realize a need for a trusted, neutral privacy program that focuses on the collection of information from children. Building on its familiarity, experience, and knowledge of the Children's Online Privacy Protection Act ("COPPA") and as the most notable privacy related infomediary service available today, Privo introduced the Privacy Assurance Program in 2003.

The Privacy Assurance Program is the first truly integrated privacy program that provides parents and children with the ability to manage their personal information that a website obtains from them, and companies with the confidence that the information they obtained from children is compliant with COPPA.

Program Requirements

Member companies must agree to abide by the Program Requirements. The Program Requirements are a set of guidelines that regulates the way member companies collect, use and disclose personal information from children 12 years old and under. By following the Program Requirements, visitors to websites operated by a member company are assured that:

- A privacy policy will be posted on the homepage of a member company website and provide a link to such privacy policy at each point within the website where personal information is collected;

- Notice will be provided to the child's parent about the website's information practices and prior verifiable consent will be obtained before collecting personal information from children;

- The child's parent will be given the choice to consent to the collection and use of their child's personal information for internal use by the website, and the parent will be given the opportunity to elect not to have their child's personal information disclosed to third parties;

- The parent will be provided with access to their child's personal information, and given the ability to delete the information and opt-out of the future collection or use of the information;

- The child's participation in an activity will not be conditioned on the child's disclosure of more personal information than is reasonably necessary for the activity; and

- Member companies will maintain the confidentiality, security, and integrity of the personal information they collect from Children.

Privo's Membership Seal of Approval

Member companies that satisfy the Program Requirements are permitted to display Privo's Seal of Approval. For parents and children, the Membership Seal of Approval offers them assurance that the website has a posted privacy policy, that the privacy policy describes how the information is collected and used, and that website submits to ongoing monitoring and enforcement of their website. Visitors to websites that are members in the Privacy Assurance Program can verify such membership by using the "click to verify" feature of the seal. Each Membership Seal of Approval is linked to a verification page on a secure Privo server. The verification page allows parents to verify that the website is authorized to display Privo's Membership Seal of Approval and is in full compliance with the Program Requirements.

Compliance Advancement Team

As part of the Program Requirements, member companies must post a privacy policy that is clear, understandable, and contains no unrelated, contradictory, or confusing material. To assist member companies with implementing a meaningful privacy policy that properly conveys to the parent and child the necessary information about the website's information practices, Privo offers its member companies guidance on how to modify their existing privacy policy, or help with

drafting their first privacy policy, to make sure that all member companies comply with the Program Requirements.

Compliance Monitoring

Compliance monitoring is a central part of the entire Privacy Assurance Program and includes the following components: initial and annual self-evaluation of a member company's website; quarterly and periodic, unannounced monitoring reviews of the member company's website; and, community monitoring reviews.

First, all member companies must conduct an initial evaluation of their website's information collection, use, and disclosure practices. Each member company is required to complete and attest to the accuracy of the statements they make on a self-evaluation form about their information practices. A representative of the Privacy Assurance Program will independently review the website's privacy policy and practices with the self-evaluation form to ensure that they are consistent with each other, the Program Requirements, and COPPA. Before becoming a participating member in the Privacy Assurance Program, the company seeking membership to the Privacy Assurance Program must make all required modifications to their website that Privo deems necessary to comply with the Program Requirements and COPPA. Member companies will be required to complete the same self-evaluation form on an annual basis to ensure that their website's information practices continually comply with the Program Requirements and COPPA, and are consistent with their posted privacy policies.

Second, all member companies must submit to quarterly monitoring of their website's information practices. The purpose of monitoring reviews is to ensure that a member company's website and its privacy policy are constantly in full compliance with the Program Requirements and COPPA. Specifically, monitoring reviews are conducted by trained privacy monitors that systematically move about a member company's website ensuring that: (i) there is prominent link to the website's privacy policy on the homepage and any web page where information is collected by the website; (ii) the member company obtains prior verifiable parental consent from all children twelve years old and under before collecting their personal information; and (iii) generally comply with the Program Requirements.

In addition to quarterly monitoring, a member company must also agree to submit to periodic, unannounced reviews of their website. These unannounced reviews will be used to further verify that the member company's website is complying with the Program Requirements and COPPA at all times. The Privacy Assurance Program will also periodically "seed" the personal information it maintains on behalf of a member company to confirm that the member company is not using the information for any other purposes than the stated purpose in its privacy policy. Each quarterly and periodic review is memorialized in a written report and maintained by the Privacy Assurance Program for a period of three (3) years.

Third, all member companies must provide the parent and child with a reasonable and effective means to submit complaints that they may have about the member company's information practices. The Privacy Assurance Program also offers the parent and child the opportunity to submit complaints about any member company website directly to the Privacy Assurance Program. A representative of the Privacy Assurance Program handles all complaints immediately. The Privacy Assurance Program maintains a record for three (3) years of all complaints received by the Privacy Assurance Program, and any investigation conducted by Privo into the alleged violation of the Program Requirements and the outcome of such investigation.

Privo Resolution Services

Member companies must provide the parent and the child with a means to submit questions or complaints that they may have about a member company's information practices. If the parent or child is not satisfied with the response they receive from the member company, the Privacy Assurance Program offers parents with assistance with resolving those complaints. Such assistance may include contacting the member company directly to investigate the complaint and finding a resolution to the parent or child's concern or requiring a representative of the member company to participate in the Privacy Assurance Program's alternative dispute resolution services. In both cases, a trained member of the Privacy Assurance Program staff administers the process.

I(B) FULL TEXT OF THE PRIVACY ASSURANCE PROGRAM REQUIREMENTS

Privo recognizes the importance of maintaining a safe and secure environment for children online. To help facilitate this type of environment for children online, Privo offers these seven requirements as guidelines that member companies must follow when operating websites directed in whole or in part to children 12 years old and under that collect information from children, or that have actual knowledge they collect information from children 12 years old and under.

Requirement 1: Notice/Disclosure of Information

Members that collect personal information from children twelve years old or under must post a prominent link that is clearly labeled *Privacy Policy* or such similar notice that links the children to a description of the Member's information collection, use, and disclosure practices.

The privacy policy link must be plainly visible on the homepage and on each web page where personal information is collected from children and in close proximity to the requests for information in each such area. For general audience websites, the privacy policy link must be

plainly visible on the first page of the children's section of the website.

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. Such information must include the name, mailing address, telephone number, and email address. In cases where more than one company is responsible for a website, the Member may choose to respond to all inquiries from parents concerning the Member's privacy policies; provided that, the names of all persons or companies collecting personal information through the website are listed.

B. Types of Personal Information Collected: Members must describe the types of personal information collected and whether the personal information is collected directly or passively.

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. If the Member does disclose personal information, the Member must: (1) describe the types of business in which such third parties are engaged and the general purposes for which the information is used; (2) whether the third parties have agreed to maintain the confidentiality, security, and integrity of the personal information they obtain from the Member; and, (3) that the parent has the option to consent to the collection and use of their child's personal information without consenting to the disclosure of that information to third parties.

E. Control Over Personal Information: Members must state in their privacy policies the choices available to the parent and the child regarding how the child's personal information is collected and used.

F. Restrictions on Information Collection: Members must state that they 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.

G. Access to Information: Members must state that parents can review the child's personal information, update the child's information, have such information deleted, and refuse to permit further collection or use of the child's information. Members must also indicate the procedures that the parent must follow to access their child's personal information.

H. Questions/Complaints: Members must state in their privacy policies where the parent or child can address any questions or complaints that they may have about the website's information practices.

Requirement 2: Direct Notice to Parents

Members must make reasonable efforts 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.

Direct Notices to Parents must contain the following information:

A. Privacy Policy Information: Members must include all of the information that is necessitated as part of *Requirement 1*, above.

B. Purpose is to Collect Information: Members must state that they wish to collect personal information from the child.

C. Parental Consent Required: Members must state that the parent's consent is required for the collection, use, or disclosure of child's personal information. Members must also provide the method by which a parent may give such consent.

Except for certain circumstances described under Requirement 3(C), Members must meet the requirements described above and obtain prior verifiable parental consent before they are allowed to collect personal information from children.

Requirement 3: 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.

B. Method for Obtaining Verifiable Parental Consent: To comply with Requirement 3 (Prior Verifiable Parental Consent), Members must obtain prior verifiable parental consent. Any method to obtain prior verifiable parental consent must be reasonably calculated,

in light of the available technology, to ensure that the person providing consent is the child's parent.

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 or facsimile; (ii) requiring the parent to use a credit card in connection with a transaction; (iii) having a parent call a toll-free telephone number staffed by trained personnel; or (iv) using the PrivoLock™ System (*See* Section 312.5 on pages 24-25 for a description of the PrivoLock™ System).

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. 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 a few exceptions where a Member will be allowed to collect a child's first name or online contact 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 to be used for the sole purpose of obtaining the 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 the first name or online contact information from a child under this exception must provide direct notice to the parent. The direct notice must include all privacy policy information (*See* Requirement 2(A), above) and notify the parent that the Member has collected the child's first name and email address to respond to and obtain consent from the parent. If the Member has not obtained parental consent after a reasonable time from the date the information is collected, the Member must delete such information from its records.

- *One-Time Request* - Members may collect the online contact information of a child for the sole purpose of responding directly, on a one-time basis, to a specific request from the child. Members that collect the 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.

- *Multiple Requests* - Members may collect the 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. Members that obtain the online contact information from a child under this exception must provide direct notice to the parent. The direct notice must: (1) include all privacy policy information (*See* Requirement 2(A), above); (2) notify the parent that the Member has collected the child's online contact information to respond to the child's request; (3) explain the nature and intended use of the information; (4) inform the parent that they may request that the Member make no further use of the information and that such information be deleted; (5) describe the procedures by which the parent can refuse to allow further contact and information collection from the child; and, (6) explain that if the parent does not opt-out, the Member may use the information for the purposes stated in the direct notice. The direct notice must be sent after the initial response and before making any additional response to the child.

- *Child Safety* - Members may collect the child's first name or online contact information to the extent reasonably necessary to protect the safety of a child participant on the website where the Member used reasonable efforts to provide notice to the parent. The information collected by a Member under this exception must be used for the sole purpose of protecting the child's safety, must not be used to re-contact the child or for any other purpose than for the purpose stated in this exception, and must not be disclosed by a Member on its website. The direct notice must: (1) include all privacy policy information (*See* Requirement 2(A), above); (2) notify the parent that the Member has collected the child's online contact information to protect the safety of the child participating on the website; (3) inform the parent that they may refuse to permit the use of the information and may require its deletion, and inform them how they can have the information deleted; and, (4) explain that if the parent does not opt-out, the Member may use the information for the purposes stated in the direct notice.

- *Additional Safety Concerns* - Members may collect a child's first name or online contact information to protect the security or integrity of its website, 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 is not required under this exception.

Requirement 4: 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 specific types of personal information collected from the child; (b) the opportunity at any time to refuse to permit the Member's further using or collecting the child's personal information; and, (c) the ability to direct the Member to delete the child's personal information from the Member's records.

In addition to 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. 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 5: 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.

Requirement 6: 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.

Requirement 7: Compliance/Enforcement

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

B. Initial and Annual Self-Evaluation: Members must conduct an evaluation of their website'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 self-evaluation form about their information practices. Once Privo receives the self-evaluation form, a Privo representative will independently review the website's posted privacy policy, information practices, and the self-evaluation form for

compliance with the Program Requirements. Once the Member's website 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 self-evaluation form on an annual basis to ensure that their website's information practices are consistent with their posted privacy policies and the Program Requirements.

C. Compliance Monitoring: Members must submit to monitoring of their website's information practices. The purpose of monitoring reviews is to ensure that a Member's privacy policy is consistent with its website's information practices. Monitoring reviews also allow Privo to verify that the Member's website complies with the Program Requirements at all times. The compliance monitoring will be conducted on a quarterly basis. In addition to the quarterly monitoring, Members must also agree to submit to periodic, unannounced reviews of their website. 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 website 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 website 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.

F. Investigations/Referral to Governmental Agencies: If Privo determines, after a thorough investigation into the Member's information practices, that a Member has violated its posted privacy policy or any of the requirements described above, Privo may refer such Member to the Federal Trade Commission for possible unfair and deceptive trade practices.

PART II: A COMPARISON OF EACH PROVISION OF SECTION 312.3 THROUGH SECTION 312.8 WITH THE CORRESPONDING PROVISIONS OF THE PROGRAM REQUIREMENTS.

Section Number	Children's Online Privacy Protection Rule	Corresponding Section of the Privacy Assurance Program Requirements
§ 312.3	**Regulation of unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the Internet.**	Under §312.3, the Final Rule sets forth the overall scheme of the Children's Online Privacy Protection Act, which is to regulate unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the Internet. Specifically, the Final Rule states under §312.3 that an operator must: ▪ Provide notice on the website or online service of what information it collect from children, how it uses such information, and disclosure practices for such information; ▪ Obtain verifiable parental consent prior to any collection, use, and/or disclosure of personal information form children; ▪ Provide a reasonable means for a parent to review the personal information collected from a child and to refuse to permit its further use or maintenance; ▪ Not condition a child's participation in a game, the offering of a prize, or another activity on the child disclosing more personal information than is reasonably necessary to participate in such activity; and,

- Establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.

Under the Privacy Assurance Program, member companies are required to adhere to and abide by this general requirement in order to prevent any possibility of unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the Internet. Specifically, member companies must comply with the following seven program requirements:

Requirement 1 (Notice/Disclosure of Information): Member companies must post a prominent link that is clearly labeled Privacy Policy or such similar notice that links the parent or child to a description of the member's information collection, use, and disclosure practices.

Requirement 2 (Direct Notice to Parents): Member companies must make reasonable efforts 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.

Requirement 3 (Prior Verifiable Parental Consent): Member companies must obtain verifiable consent before any collection, use, or disclosure of personal information from children unless permitted to collect the child's name or online contact information under one of the exceptions to prior verifiable parental consent set forth in §312.5(c) of the Final Rule.

Requirement 4 (Access and Review): Member companies must provide parents with the ability to access and review their child's personal information.

		Requirement 5 (Restrictions on Information Collection): Member companies must not condition a child's participation in an activity on the child's disclosing more personal information than is reasonably necessary to participate in such activity. **Requirement 6 (Confidentiality, Security and Integrity of Information):** Member companies must establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children. **Requirement 7 (Compliance and Enforcement):** Member companies must implement effective and meaningful compliance and enforcement mechanisms that ensure that they comply with their information policies and practices.
§ 312.4	**Notice.**	**Requirement 1: <u>Notice/Disclosure of Information</u>** Members that collect personal information from children twelve years old or under must post a prominent link that is clearly labeled *Privacy Policy* or such similar notice that links the children to a description of the Member's information collection, use, and disclosure practices. The privacy policy link must be plainly visible on the homepage and on each web page where personal information is collected from children and in close proximity to the requests for information in each such area. For general audience websites, the privacy policy link must be plainly visible on the first page of the children's section of the website. 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. Such information must include the name, mailing address, telephone number, and email address. In cases where more than one company is responsible for a website, the Member may choose to respond to all inquiries from parents concerning the Member's privacy policies; provided that, the names of all persons or companies collecting personal information through the website are listed.

B. Types of Personal Information Collected: Members must describe the types of personal information collected and whether the personal information is collected directly or passively.

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. If the Member does disclose personal information, the Member must: (1) describe the types of business in which such third parties are engaged and the general purposes for which the information is used; (2) whether the third parties have agreed to maintain the confidentiality, security, and integrity of the personal information they obtain from the Member; and, (3) that the parent has the option to consent to the collection and use of their child's personal information without consenting to the disclosure of that information to third parties.

E. Control Over Personal Information: Members must state in their privacy policies the choices available to the parent and the child regarding how the child's personal information is collected and used.

F. Restrictions on Information Collection: Members must state that they 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.

G. Access to Information: Members must state that parents can review the child's personal information, update the child's information, have such information deleted, and refuse to permit further collection or use of the child's information. Members must also indicate the procedures that the parent must follow to access their child's personal information.

H. Questions/Complaints: Members must state in their privacy policies where the parent or child can address any questions or complaints that they may have about the website's information practices.

§ 312.5	Parental consent.	**Requirement 3: 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. B. Method for Obtaining Verifiable Parental Consent: To comply with Requirement 3 (Prior Verifiable Parental Consent), Members must obtain prior verifiable parental consent. Any method to obtain prior verifiable parental consent must be reasonably calculated, in light of the available technology, to ensure that the person providing consent is the child's parent. 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 or facsimile; (ii) requiring the parent to use a credit card in connection with a transaction; (iii) having a parent call a toll-free telephone number staffed by trained personnel; or (iv) using the PrivoLock™ System. 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.

§ 312.6	**Right of parent to review personal information provided by a child.**	**Requirement 4: <u>Access and Review</u>** 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 specific types of personal information collected from the child; (b) the opportunity at any time to refuse to permit the Member's further using or collecting the child's personal information; and, (c) the ability to direct the Member to delete the child's personal information from the Member's records. In addition to 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. 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.).
§ 312.7	**Prohibition against conditioning a child's participation on collection of personal information.**	**Requirement 5: <u>Restrictions on Information Collection</u>** 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.

§ 312.8	**Confidentiality, security, and integrity of personal information collected from children.**	**Requirement 6: <u>Confidentiality, Security and Integrity of Information</u>** Members must establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.

PART III: STATEMENT EXPLAINING (A) HOW THE PROGRAM REQUIREMENTS AND ITS APPLICABLE ASSESSMENT MECHANISM MEETS THE REQUIREMENTS OF THE FINAL RULE, (B) HOW THE ASSESSMENT MECHANISM AND COMPLIANCE INCENTIVES REQUIRED UNDER SECTION 312.10(B)(2) AND (3) PROVIDE EFFECTIVE ENFORCEMENT OF THE REQUIREMENTS OF THE FINAL RULE.

III(A) How the Program Requirements and its Applicable Assessment Mechanism meets the requirements of the Final Rule.

The Program Requirements and applicable assessment mechanisms meet and exceed the requirements of §312.10. The Program Requirements were modeled on the Organisation for Economic Co-Operation and Development's ("OECD") principles of fair information practices, the Children's Online Privacy Protection Act, and the requirements enunciated in the Final Rule. The Program Requirements were drafted to mirror §§312.2 through 312.9 of the Final Rule. Therefore, member companies participating in the Privacy Assurance Program are assured that by implementing the Program Requirements they are providing the same or greater protections for children as those contained in the Final Rule. Specifically:

Section 312.2 (Defined Terms) - The Privacy Assurance Program ensures that all defined terms described in §312.2 of the Final Rule are adhered to because the Final Rule's definitions have been incorporated by reference into the Membership Agreement. As a result, member companies participating in the Privacy Assurance Program are required to read the Program Requirements in a manner that is consistent with §312.2 of the Final Rule.

Section 312.3 (General Requirements) - Under §312.3, the Final Rule sets forth the overall scheme of the Children's Online Privacy Protection Act, which is to regulate unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the Internet. Specifically, the Final Rule states under §312.3 that an operator must:

- Provide notice on the website or online service of what information it collect from children, how it uses such information, and disclosure practices for such information;
- Obtain verifiable parental consent prior to any collection, use, and/or disclosure of personal information form children;
- Provide a reasonable means for a parent to review the personal information collected from a child and to refuse to permit its further use or maintenance;
- Not condition a child's participation in a game, the offering of a prize, or another activity on the child disclosing more

personal information than is reasonably necessary to participate in such activity; and,

- Establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.

Under the Privacy Assurance Program, member companies are required to adhere to and abide by this general requirement in order to prevent any possibility of unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the Internet. Specifically, member companies must comply with the following seven program requirements:

Requirement 1 (Notice/Disclosure of Information): Member companies must post a prominent link that is clearly labeled Privacy Policy or such similar notice that links the parent or child to a description of the member company's information collection, use, and disclosure practices.

Requirement 2 (Direct Notice to Parents): Member companies must make reasonable efforts to ensure that a parent of a child receives notice of the member company'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.

Requirement 3 (Prior Verifiable Parental Consent): Member companies must obtain verifiable consent before any collection, use, or disclosure of personal information from children unless permitted to collect the child's first name or online contact information under one of the exceptions to prior verifiable parental consent set forth in §312.5(c) of the Final Rule.

Requirement 4 (Access and Review): Member companies must provide parents with the ability to access and review their child's personal information.

Requirement 5 (Restrictions on Information Collection): Member companies must not condition a child's participation in an activity on the child's disclosing more personal information than is reasonably necessary to participate in such activity.

Requirement 6 (Confidentiality, Security and Integrity of Information): Member companies must establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.

Requirement 7 (Compliance and Enforcement): Member companies must implement effective and meaningful compliance and enforcement

mechanisms that ensure that they comply with their information policies and practices.

Section 312.4 (Notice) - The Program Requirements meet the Final Rule's requirement under §312.4 that an operator of a website directed to children post a link to a notice of its information practices with regard to children on the homepage of its website and at each area on the website where personal information is collected from children. The notice of the member company's information practices must be clear and understandable, and should not contain unrelated, contradictory, or confusing material.

Specifically, the Program Requirements mandate that member companies post a privacy policy that states: (i) member company's contact information; (ii) the types of personal information collected by the member company; (iii) how the member company uses the personal information; (iv) whether the member company discloses personal information it obtains from the child; (v) what form of control the parent or child has over their personal information; (vi) any restrictions on information collection which member companies must abide by when participating in the program; (vii) how a parent or child can access and review their information; and, (viii) where a parent or child can submit a question or complaint to the member company about its website's information policies or practices.

In addition to the seven program requirements that member companies must follow when participating in the Privacy Assurance Program, each member company must also adhere to the provisions of the Membership Agreement that regulate the size, location and operation of the privacy policy link. These requirements are described in detail in the Membership Agreement and state in part as follows:

> *"Member shall display the Mark shown in Exhibit B on its Privacy Policy in a location, format and manner reasonably prescribed by Privo. Such Mark shall be part of a graphical user interface, provided by Privo, and shall activate a Link that shall directly access a Privo server for authentication purposes."*

Section 312.5 (Prior Verifiable Parental Consent) - The Program Requirements meet the Final Rule's requirement under §312.5. Specifically, under Requirement 3(A) of the Program Requirements, member companies must obtain verifiable parental consent before any collection, use, or disclosure of personal information from children. Member companies must also obtain such consent to any material change in the collection, use, or disclosure practices to which the parent has previously consented.

Moreover, under Requirement 3(B), member companies must obtain prior verifiable parental consent. Such methods to obtain prior verifiable parental consent may include: (i) providing a consent form to be signed by the parent and returned to the member company by

postal mail or facsimile; (ii) requiring the parent to use a credit card in connection with a transaction; (iii) having a parent call a toll-free telephone number staffed by trained personnel; or (iv) using one of the online or offline verification methods of the PrivoLock™ System.

The PrivoLock™ System is a suite of online and offline methods by which an individual can authenticate their identity and therefore activate their account in order to provide member sites with verifiable permission. The PrivoLock™ System currently provides five (5) methods of verification. The online mechanisms include: (i) the verification of the last four digits of the individual's social security number; (ii) verification of the individual's driver's license number; and, (iii) the use of a credit card in connection with a transaction. The offline methods include (i) printing out a parental consent form, signing it, and mailing or faxing the form to the Privacy Assurance Program or (ii) providing consent over the telephone using a toll free number staffed by trained operators.

The PrivoLock™ System is an efficient and effective means for a parent to give permission to a member company's website that wishes to collect personal information from the parent's child. In most cases, the online verification process only takes a few minutes to complete; the offline methods may take from 3-5 days.

The need for parental consent is triggered when the child first attempts to register at the website and is immediately greeted by a "gate" in which he/she must provide their birth-date. Upon entering information that indicates the child is under 13, the child is directed to contact a parent or teacher.

At this point the adult begins the verification process. The first step is for the parent or teacher to register with the website using the PrivoLock™ System. Prior to actually completing the adult registration form, the parent or teacher will be given notice of the website's information collection, use, and disclosure practices with regard to their child in accordance with Requirement 2 of the Program Requirements and COPPA. Once the parent has read the Direct Notice to Parent, the parent is prompted to complete the adult registration.

The next step is to verify that the individual providing consent is an adult by one of the five (5) methods of verification mentioned above. Verification entails submitting the data provided by the adult against the appropriate database and determining whether there is a match.

If the parent successfully verifies using one the methods described above, the parent will then be able to provide consent for the account that their child has already initiated or, if the parent has not registered their child but would like to, set-up a new account for their child. The Parent will also be able to actively manage their child's account information, including what website features

their child can participate in or whether they can receive information such as newsletters from the member company.

Furthermore, where a website is solely directed to children 12 years old or under and does not provide a "gate" in which the individual must provide their birth-date, a member company must assume that the individual is a child and obtain verifiable consent from that individual's parent before collecting, using, or disclosing their personal information.

Lastly, even though prior verifiable parental consent is required under most situations before a member company is permitted to collect, use, or disclose a child's personal information, there are a few exceptions where a member company is permitted to collect a child's first name or online contact information before obtaining consent from the child's parent. In such circumstances, member companies must comply with Requirement 3(C) of the Program Requirement, which describes the exceptions to prior verifiable parental consent and is consistent with the Final Rule's requirement under §312.5(c).

Consistent with §312.5 of the Final Rule, member companies are also required to 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.

Section 312.6 (Right of Parent to Review Personal Information Provided by a Child) - The Program Requirements meet the Final Rule's requirement under §312.6, which states that upon request of a parent whose child has provided personal information to a website that such website provide the parent with an opportunity to access and review their child's personal information. Specifically, under Requirement 4 of the Privacy Assurance Program, member companies are required to provide parents with the ability to access and review their child's personal information. Parental access and review must consist of: (i) a description of the specific types of personal information collected from the child; (ii) the opportunity at any time to refuse to permit the company's further using or collecting the child's personal information; and, (iii) the ability to direct the company to delete the child's personal information from the company's records.

Section 312.7 (Prohibition Against Conditioning a Child's Participation on Collection of Personal Information) - The Program Requirements meet the Final Rule's requirements of §312.7, which prohibits an operator of a website against conditioning a child's participation on collection of personal information. The Privacy Assurance Program recognizes that many websites may require a child provide their personal information to participate in activities on the website such as games, contests, or sweepstakes. And although the Privacy Assurance Program does not limit such practices, member companies are required to restrict the amount of information they collect about the child.

Specifically, under Requirement 5 of the Privacy Assurance Program, member companies 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. Member companies must also continually re-evaluate whether a valid reason exists for the information to be collected. And if the valid reason ceases to exist, member companies must restrict their collection practices in view of their revised business model.

Section 312.8 (Confidentiality, Security, and Integrity of Personal Information Collected from Children) - The Program Requirements meet the Final Rule's requirements of §312.8 by mandating that all member companies establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children. For example, member companies must implement 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.

Section 312.9 (Enforcement) - The Privacy Assurance Program compliance and enforcement mechanisms meet the Final Rule's requirements as enunciated in §312.9. Member companies are required to institute internal control mechanisms. Specifically, these mechanisms include appointing a representative of the member company that is responsible for handling all questions or complaints received from parents or children that use its website. Such representative must be given the full authority to receive and actively respond to any privacy related inquiries. If a member company has not adequately responded to a parent or child's inquiry, the member company must provide a means for the parent or child to appeal to a higher management level. In the event the parent or child remains unsatisfied with the member company's response, the member company is required to refer the parent or child to the Privacy Assurance Program.

In addition to these internal control mechanisms, the Privacy Assurance Program also requires member companies to adhere to Requirement 7. Under the Compliance and Enforcement Requirement, member companies agree to submit to compliance monitoring and shall cooperate in all respects with the Privacy Assurance Program's monitoring of the member company's compliance with the terms and conditions set forth in the Membership Agreement.

Specifically, the Membership Agreement states in part that:

> "Privo may itself, or through an independent third party designated by Privo, conduct compliance reviews from time to time of Member's information practices, implementation of Member's Privacy Policy, and operation of the Website, which reviews may be initiated in response to User complaints or for any other reason. Such reviews may include initial and periodic reviews of Member's Website,

tracking of data in Member's database via its Website, and on-site and off-site compliance reviews."

Moreover, member companies must provide the parent and the child with reasonable and effective means to submit complaints that they may have about a member companies' information practices. The Privacy Assurance Program's compliance and enforcement mechanisms are discussed in further detail below.

III(B) HOW THE ASSESSMENT MECHANISM AND COMPLIANCE INCENTIVES REQUIRED UNDER SECTION 312.10(B)(2) AND (3) PROVIDE EFFECTIVE ENFORCEMENT OF THE REQUIREMENTS OF THE FINAL RULE.

Mandatory mechanism for the independent assessment of a subject operators' compliance with the guidelines. The Privacy Assurance Program meets the requirements of §312.10(b)(2) of the Final Rule. Section 312.10(b)(2) states that an effective, mandatory mechanism for the independent assessment of a member company's compliance with the Program Requirements is required. The Privacy Assurance Program accomplishes this requirement in a number of ways, including the following:

Initial and Annual Self-Evaluation - Member companies must conduct an evaluation of their website's information collection, use, and disclosure practices. Each member company is required to complete and attest to the accuracy of the statements they make on a self-evaluation form about their information practices. Once the member company sends the self-evaluation form to the Privacy Assurance Program, a representative of the Privacy Assurance Program will independently review the self-evaluation form in conjunction with its website's actual practices to make sure what is stated in the self-evaluation form is consistent with such practices and the Program Requirements.

The independent review will consist of three steps. The first step is for a trained privacy monitor to systematically evaluate the responses made by the member company in its self-evaluation form, one question at a time, with the notice and disclosure statements contained in its posted privacy policy. Any inaccuracies found in the privacy policy must be modified to accurately reflect the member company's actual information practices before the Privacy Assurance Program will issue a Seal of Approval for that particular website.

The second step is for trained privacy monitor to review the member company's website and compare the website review with the member company's self-evaluation form and posted privacy policy to ensure that the privacy policy accurately depicts the collection practices of the website.

The third step is for a trained privacy monitor to conduct a review of the website's collection and use practices. During this segment of the website review process, a privacy monitor will submit

fictitious personal information at each point within the website where information is collected and then track that information to determine whether the member company is using the personal information they have obtained in conformity with their stated privacy policy. If personal information is collected from children twelve years old or under, then the privacy monitor verifies that prior verifiable parent consent is obtained before the child's personal information is collected by the website.

In the event the member company's website 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. To ensure that member companies remain in full compliance, each member must submit to the procedures described above on an annual basis. This allows the Privacy Assurance Program to make sure that the website is in full compliance with Program Requirements and COPPA before renewing the website's membership in the Privacy Assurance Program for an additional year.

Compliance Monitoring - Member companies must submit to quarterly and periodic, unannounced monitoring reviews of their website's information practices. The purpose of these monitoring reviews is to ensure that a member company's privacy policy is consistent with its website's information practices. Monitoring reviews also allow the Privacy Assurance Program to verify that the member's website complies with the Program Requirements and COPPA at all times.

All member companies must submit to quarterly monitoring reviews of their website's information practices. These monitoring reviews will be conducted at a minimum of once per quarter or four times per year. Specifically, monitoring reviews are conducted by trained privacy monitors that systematically move about a member company's website ensuring that: (i) there is prominent link to the website's privacy policy on the homepage and any web page where information is collected by the website; (ii) the member company obtains prior verifiable parental consent from all children twelve years old and under before collecting their personal information; and (iii) the website generally complies with the Program Requirements.

In addition to the quarterly monitoring, member companies must also agree to submit to periodic, unannounced monitoring reviews of their website. Periodic, unannounced monitoring reviews will also be conducted at a minimum of one per quarter or four times per year. These periodic, unannounced reviews will be used to further verify that the member company remains in full compliance with the Program Requirements. During these monitoring reviews, the Privacy Assurance Program randomly checks each participating website's privacy practices.

These random checks are similar to the reviews done during the quarterly monitoring with the additional element of "seeding." As mentioned previously, the Privacy Assurance Program will also

periodically "seed" the personal information the member company website has collected. In other words, the privacy monitor will submit fictitious information into its database that it maintains on behalf of a member company to track how the member company uses the personal information it has collected. These periodic reviews are another way that the Privacy Assurance Program can insure that the member company is adhering to its website's posted privacy policy.

Quarterly and periodic reviews are memorialized in a written report and maintained by the Privacy Assurance Program for a period of three (3) years.

Consumer Complaints/Monitoring - Member companies must provide the parent and the child with reasonable and effective means to submit complaints that they may have about a member companies' information practices. The Privacy Assurance Program also offers the parent or child the opportunity to submit complaints about any member company directly to the Privacy Assurance Program. A Privacy Assurance Program representative responds to all complaints immediately.

Effective incentives for subject operator's compliance with the guidelines. Section 312.10(b)(3) of the Final Rule requires the Privacy Assurance Program to provide effective incentives for it member companies to ensure full compliance with the Program Requirements. This requirement is met in the following manner:

Membership Agreement Obligations - Member companies must execute the Privacy Assurance Program membership agreement. As part of this agreement, member companies must agree to comply with these Program Requirements at all times. In the event that a member company 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.

Consumer Complaints/Monitoring - Member companies shall create and implement effective and affordable mechanisms that ensure compliance with its Privacy Policy and provide appropriate means of resolving consumer complaints. Such mechanisms for resolving consumer complaints include the appointment of at least one individual to whom a parent or child can bring inquiries regarding member company's privacy practices. The designated individual must be given the authority by the member company to investigate all inquiries or complaints and complete this investigation in a timely manner, but in no event later than fourteen (14) business days.

The member company is required to cooperate with the Privacy Assurance Program's efforts to resolve complaints, questions, or concerns on behalf of a parent or child. In the event a parent or child is not satisfied with the means of recourse provided by member company and/or the resolution of a complaint, the member company is required to refer the individual to the Privacy Assurance Program.

If the Privacy Assurance Program determines that a violation of the requirements has occurred, the member company is informed of such violation and the corrective actions that must be taken to bring the member company's website into compliance. Failure to take the corrective actions can result in a number consequences including removal from the Privacy Assurance Program (as described above under Membership Agreement obligations) and referral to the appropriate governmental agency (as described below under Referral to the Commission).

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

Referral to the Commission - If the Privacy Assurance Program determines, after a thorough investigation into the member company's information practices, that a member company has violated its posted privacy policy or any of the Program Requirements, the Privacy Assurance Program is prepared to refer such member company to the Commission for possible unfair and deceptive trade practices.

IV. Conclusion

Privo commends the Commission for its outstanding work in the area of children's privacy. Privo appreciates this opportunity to demonstrate to the Commission that its Privacy Assurance Program Requirements meet the requirements of the Final Rule. It is our belief that the Privacy Assurance Program, the Membership Agreement, the Compliance and Enforcement mechanisms, PrivoLock™ System, and the individualized counseling we make available to member companies will provide an effective self-regulatory program for protecting the personal information of children online.

Privacy Assurance Program

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

Privo recognizes the importance of maintaining a safe and secure environment for children online. To help facilitate this type of environment for children online, Privo offers these seven requirements as guidelines that companies must follow when operating websites directed in whole or in part to children 12 years old and under that collect information from children, or that have actual knowledge they collect information from children 12 years old and under.

Specifically, companies that are participants in the Privacy Assurance Program ("Members") must comply with the rules and regulations contained in the 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"). In addition, Members must implement each of the seven requirements described below:

Requirement 1: Notice/Disclosure of Information

Members that collect personal information from children twelve years old or under must post a prominent link that is clearly labeled *Privacy Policy* or such similar notice that links the children to a description of the Member's information collection, use, and disclosure practices.

The privacy policy link must be plainly visible on the homepage and on each web page where personal information is collected from children and in close proximity to the requests for information in each such area. For general audience websites, the privacy policy link must be plainly visible on the first page of the children's section of the website.

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. Such information must include the name, mailing address, telephone number, and email address. In cases where more than one company is responsible for a website, the Member may choose to respond to all inquiries from parents concerning the Member's privacy policies; provided that, the names of all persons or companies collecting personal information through the website are listed.

B. Types of Personal Information Collected: Members must describe the types of personal information collected and whether the personal information is collected directly or passively.

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. If the Member does disclose personal information, the Member must: (1) describe the types of business in which such third parties are engaged and the general purposes for which the information is used; (2) whether the third parties have agreed to maintain the confidentiality, security, and integrity of the personal information they obtain from the Member; and, (3) that the

parent has the option to consent to the collection and use of their child's personal information without consenting to the disclosure of that information to third parties.

E. Control Over Personal Information: Members must state in their privacy policies the choices available to the parent and the child regarding how the child's personal information is collected and used.

F. Restrictions on Information Collection: Members must state that they 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.

G. Access to Information: Members must state that parents can review the child's personal information, update the child's information, have such information deleted, and refuse to permit further collection or use of the child's information. Members must also indicate the procedures that the parent must follow to access their child's personal information.

H. Questions/Complaints: Members must state in their privacy policies where the parent or child can address any questions or complaints that they may have about the website's information practices.

Requirement 2: Direct Notice to Parents

Members must make reasonable efforts 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.

Direct Notices to Parents must contain the following information:

A. Privacy Policy Information: Members must include all of the information that is necessitated as part of *Requirement 1*, above.

B. Purpose is to Collect Information: Members must state that they wish to collect personal information from the child.

C. Parental Consent Required: Members must state that the parent's consent is required for the collection, use, or disclosure of child's personal information. Members must also provide the method by which a parent may give such consent.

Except for certain circumstances described under Requirement 3(C), Members must meet the requirements described above and obtain prior verifiable parental consent before they are allowed to collect personal information from children.

Requirement 3: 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.

B. Method for Obtaining Verifiable Parental Consent: To comply with Requirement 3 (Prior Verifiable Parental Consent), Members must obtain prior verifiable parental consent. Any method to obtain prior verifiable parental consent must be reasonably calculated, in light of the available technology, to ensure that the person providing consent is the child's parent.

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 or facsimile; (ii) requiring the parent to use a credit card in connection with a transaction; (iii) having a parent call a toll-free telephone number staffed by trained personnel; or (iv) using the PrivoLock™ System.

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. 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 a few exceptions where a Member will be allowed to collect a child's first name or online contact 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 to be used for the sole purpose of obtaining the 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 the first name or online contact information from a child under this exception must provide direct notice to the parent. The direct notice must include all privacy policy information (*See* Requirement 2(A), above) and notify the parent that the Member has collected the child's first name and email address to respond to and obtain consent from the parent. If the Member has not obtained parental consent after a reasonable time from the date the information is collected, the Member must delete such information from its records.

- *One-Time Request* – Members may collect the online contact information of a child for the sole purpose of responding directly, on a one-time basis, to a specific request from the child. Members that collect the 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.

- *Multiple Requests* – Members may collect the 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. Members that obtain the online contact information from a child under this exception must provide direct notice to the parent. The direct notice must: (1) include all privacy policy information (*See* Requirement 2(A), above); (2) notify the parent that the Member has collected the child's online contact information to respond to the child's request; (3) explain the nature and intended use of the information; (4) inform the parent that they may request that the Member make no further use of the information and that such information be deleted; (5) describe the procedures by which the parent can refuse to allow further contact and information collection from the child; and, (6) explain that if the parent does not opt-out, the Member may use the information for the purposes stated in the direct notice. The direct notice must be sent after the initial response and before making any additional response to the child.

- *Child Safety* – Members may collect the child's first name or online contact information to the extent reasonably necessary to protect the safety of a child participant on the website where the Member used reasonable efforts to provide notice to the parent. The information collected by a Member under this exception must be used for the sole purpose of protecting the child's safety, must not be used to re-contact the child or for any other purpose than for the purpose stated in this exception, and must not be disclosed by a Member on its website. The direct notice must: (1) include all privacy policy information (*See* Requirement 2(A), above); (2) notify the parent that the Member has collected the child's online contact information to protect the safety of the child participating on the website; (3) inform the parent that they

may refuse to permit the use of the information and may require its deletion, and inform them how they can have the information deleted; and, (4) explain that if the parent does not opt-out, the Member may use the information for the purposes stated in the direct notice.

- *Additional Safety Concerns* – Members may collect a child's first name or online contact information to protect the security or integrity of its website, 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 is not required under this exception.

Requirement 4: 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 specific types of personal information collected from the child; (b) the opportunity at any time to refuse to permit the Member's further using or collecting the child's personal information; and, (c) the ability to direct the Member to delete the child's personal information from the Member's records.

In addition to 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. 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 5: 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.

Requirement 6: 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.

Requirement 7: Compliance/Enforcement

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

B. Initial and Annual Self-Evaluation: Members must conduct an evaluation of their website'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 self-evaluation form about their information practices. Once Privo receives the self-evaluation form, a Privo representative will independently review the website's posted privacy policy, information practices, and the self-evaluation form for compliance with the Program Requirements. Once the Member's website 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 self-evaluation form on an annual basis to ensure that their website's information practices are consistent with their posted privacy policies and the Program Requirements.

C. Compliance Monitoring: Members must submit to monitoring of their website's information practices. The purpose of monitoring reviews is to ensure that a Member's privacy policy is consistent with its website's information practices. Monitoring reviews also allow Privo to verify that the Member's website complies with the Program Requirements at all times. The compliance monitoring will be conducted on a quarterly basis. In addition to the quarterly monitoring, Members must also agree to submit to periodic, unannounced reviews of their website. 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 website 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 website 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.

F. Investigations/Referral to Governmental Agencies: If Privo determines, after a thorough investigation into the Member's information practices, that a Member has violated its posted privacy policy or any of the requirements described above, Privo may refer such Member to the Federal Trade Commission for possible unfair and deceptive trade practices.

Privacy Assurance Program

Monitoring Review Report

Website Name: _____

Website URL: _____

Company Name: _____

Contact Name: _____

Date Reviewed: _____

PRIVACY POLICY:

1. **Does the website have a prominent privacy policy link displayed on its homepage?** ☐ **Yes** ☐ **No**

2. **Does the privacy policy link to the website's privacy policy?** ☐ **Yes** ☐ **No**

3. **Is a privacy policy link displayed on all web pages where personal information is collected?** ☐ **Yes** ☐ **No**

4. **Does the website's privacy policy include the following information? Please place a check next to the information contained in the website's privacy policy and attached a copy of the website's privacy policy to this report.**

   ☐ Company's complete contact information
   ☐ Types of personal information the website collects
   ☐ How the website will use the information it collects
   ☐ How the website discloses the information that it collects
   ☐ The choices available to the parent and child with regard to how their personal information may be used
   ☐ Whether the website prohibits the conditioning a child's participation in an activity on the child's disclosing more personal information than is necessary
   ☐ How the parent or child can access their personal information
   ☐ Where the parent or child can address any questions or complaints that they may have regarding your website

WEBSITE:

5. **Does the website collect personal information from children under 13?**
   ☐ Yes ☐ No

6. **What types of personal information does the website collect from the child or the parent of that child?**

   ☐ First name
   ☐ Last name
   ☐ Mailing address
   ☐ Email address
   ☐ Telephone number
   ☐ Credit card number and expiration date
   ☐ Last four digits of the parent's social security number
   ☐ Other, please explain further:

   _____

   _____

7. **Does the website request parental consent before obtaining personal information from children under 13?** ☐ Yes ☐ No

8. **What method of parental consent does the website employ?**

   ☐ Sign, print, and send method
   ☐ 1-800-Number supported by trained personnel
   ☐ PrivoLock™ System
   ☐ Other, please describe further:

   _____

   _____

9. **Does the website provide Direct Notice to Parents at the time they obtain parental consent?** ☐ Yes ☐ No

10. What type of information does the Direct Notice to Parents contain?

- ☐ All information contained in the privacy policy
- ☐ A statement notifying the parent that the website wishes to collect personal information form the child and cannot do so without prior verifiable parental consent
- ☐ A statement that the parent can consent to the website's collection and internal use of personal information without consenting to the disclosure of that information to third parties
- ☐ A statement about how the parent can limit disclosure of their child's personal information

11. Does the website collect demographic information? ☐ Yes ☐ No (If yes, please select all that apply)

- ☐ Username and password
- ☐ Date of birth or age
- ☐ Gender
- ☐ Hobbies and interests
- ☐ Other, please describe further:

_____

_____

12. Does the website feature message boards, chat rooms, or other interactive features where a child's personal information can be publicly disclosed? ☐ Yes ☐ No

Please describe the types of interactive features contained on the website:

_____

_____

_____

_____

13. Does the website use passive collection mechanisms? ☐ Yes ☐ No

14. **Which passive collection mechanisms does the website use?**

- ☐ Cookies
- ☐ Clear GIFs
- ☐ Other, please describe further:

_____

_____

15. **Does the website link to other websites on the World Wide Web?** ☐ Yes ☐ No

16. **Does the website include a bumper screen or a notice that warns the user that they are leaving the current website and that the website's privacy policy no longer applies?** ☐ Yes ☐ No

17. **Does the website provide the parent or the child with the ability to make a choice about how their personal information will be used?** ☐ Yes ☐ No (If yes, please indicate what type of choices)

What type of choice does the website offer?

- ☐ The website offers users the opportunity to opt-out of an activity or from receiving information
- ☐ The website offers users the opportunity to opt-in to an activity or to receiving information from our company or other permitted entities
- ☐ The website offers users with either the opportunity to opt-in or opt-out depending on the activity
- ☐ Other, please describe further:

_____

_____

18. **Please describe any general concerns or comments about the website:**

_____

_____

_____

_____

IF YOU ARE CONDUCTING A PERIODIC, UNANNOUNCED MONITORING REVIEW, PLEASE FOLLOW THE DIRECTIONS BELOW:

SEEDING INFORMATION:

Please complete all registrations or forms on the website. The privacy monitor will provide you with the necessary fictitious information, including the name, address and email address.

Insert the fictitious information used during your monitoring review session in the space provided:

Child's Name: _____

Child's Email Address: _____

Parent's Name: _____

Parent's Email Address: _____

Mailing Address: _____

_____

PRIVO Privacy Assurance Program Membership Agreement

[Redacted From Public Record Version]

PRIVO Privacy Assurance Program Self-Evaluation Form

[Redacted From Public Record Version]