



May 1, 2000

Donald S. Clark, Secretary of the Commission
Federal Trade Commission
600 Pennsylvania Ave, N.W.
Washington, D.C. 20580

RE: Request for Safe Harbor Seal Program Status by the Federal Trade Commission ("FTC") for the ESRB Privacy Online Principles and Guidelines for Fair Information Practices under § 312.10 of the Children's Online Privacy Protection Rule.

Dear Secretary Clark:

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), ESRB Privacy Online, a division of the Entertainment Software Rating Board ("ESRB"), respectfully submits the following application for approval as a safe harbor privacy seal program within the meaning of the Final Rule §312.10 implementing the Children's Online Privacy Protection Act (15 U.S.C. 6501 et seq.).

The following application is divided into three (3) sections:

Section I provides: (i) accompanying commentary regarding ESRB, the establishment of the ESRB Privacy Online Program and the general services the ESRB Privacy Online Program offers (*Section I(A)*); and, (ii) the full text of the ESRB Privacy Online Principles and Guidelines for which approval is sought (*Section I(B)*).

Section II contains a provision comparison chart. As requested, this section provides a comparative analysis of each provision of §§312.3 through 312.8 with the corresponding provisions of the ESRB Privacy Online Principles and Guidelines.

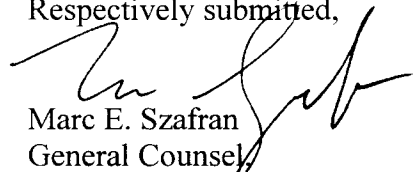
Section III provides a statement explaining: (i) how the ESRB Privacy Online Principles and Guidelines, including the applicable assessment mechanism, meet the requirements of the Final Rule as requested in §312.10 (*Section III(A)*); and, (ii) how the assessment mechanism and

E**B**

compliance incentives required under §§312.10 (b)(2) and (3) provide effective enforcement of the requirements set forth in the Final Rule (*Section III(B)*).

ESRB Privacy Online is pleased to submit this application to the FTC. We look forward to working with the FTC during your review process and can provide any additional information that would be helpful to the Commission. We thank you in advance for your consideration.

Respectfully submitted,



Marc E. Szafran
General Counsel
ESRB Privacy Online

1111

B

SECTION I



SECTION I – COPY OF THE FULL TEXT OF THE ESRB PRIVACY ONLINE PRINCIPLES AND GUIDELINES AND ACCOMPANYING COMMENTARY.

I(A) - Accompanying Commentary.

Introduction

The ESRB Privacy Online Program is an independent privacy seal program that assists companies in protecting consumer personal information collected online. Our program helps guard the rights of Web consumers, and the interests of Web publishers, and makes the Internet a secure, reliable, and private place to share information and conduct business. From our principles and guidelines for fair information practices, to our policy guidance and statement creation team, to our Sentinel enforcement mechanisms, we offer the most comprehensive and effective privacy seal provider service available today.

Background

ESRB Privacy Online is a division of the Entertainment Software Rating Board (“ESRB”), an independent, self-regulatory entity that has developed a standardized rating system for all entertainment software, including computer and video games. Established in 1994, today the ESRB is the nation's leading, non-profit, entertainment software rating body for the interactive entertainment software industry. As of February 2000, the ESRB has rated over 6,500 titles submitted by over 350 of the industry's leading publishers. Building on the experience, knowledge, and success of ESRB and *ESRBinteractive*—another successful self-regulatory body within the online industry—ESRB launched the ESRB Privacy Online Program in June of 1999. As an independent, third party privacy seal provider, ESRB Privacy Online seeks to ensure that consumers’ experiences online are as safe, private, reliable and secure as possible.

ESRB Privacy Online Program Requirements

Participating companies must adhere to rigorous ESRB Privacy Online Program requirements, including accepted Principles and Guidelines for Fair Information Practices (“Principles and Guidelines”). The Principles and Guidelines regulate online information collection and use practices by requiring participating companies to maintain a commitment to consumer notice, consumer choice, data access, children’s privacy protection, and data integrity. Compliance with the ESRB Privacy Online Program requires companies to display the ESRB Privacy Online Certification Seal on their homepage, all main pages, and any information entry points where a consumer could disclose their identity or personal information. This ensures that:

- Web users are given clear and simple notice of a site’s information practices;
- Web users have options regarding whether and how their personal information is used;



- Web users have reasonable access to information about them collected online and have the opportunity to correct any inaccuracies;
- Web users have assurances regarding the accuracy and security of personal information; and,
- Parents of children 12 and under can decide whether their child's information is collected and how it can be used.

The ESRB Privacy Online Seal

Companies that meet ESRB Privacy Online's high standards are awarded the prestigious ESRB Privacy Online Certification Seal — a symbol of integrity and compliance. For the Web consumer, this seal offers an assurance that the site has adopted an approved privacy policy, that its stated privacy practices are being implemented as represented in their policy statement, and that the site submits to ongoing, independent, third-party monitoring and oversight mechanisms. Each Certification Seal includes a “click-to-confirm” option that automatically links a user to ESRB Privacy Online's Authentication Page. The Authentication Page provides consumers with the ability to confirm that the site with which they are interacting is using a valid, certified ESRB Privacy Online Certification Seal and that the company is a participant in good standing with our program.

Policy Statement Creation

Because participating companies must implement and publish privacy statements that inform consumers about its information practices, ESRB Privacy Online offers services to assist companies in creating or modifying these critical documents. These services include: (i) an online privacy statement composition program called the ESRB Privacy Statement Composer; and, (ii) a Policy/Statement Creation Assistance Team.

If a participating company does not have a privacy statement, the Composer helps a company create their first draft. This draft can subsequently be customized to meet a particular business model and unique privacy practices. The Composer provides companies with the framework for creating a compliant privacy statement that gives consumers notice regarding information collection practices and demonstrates a meaningful commitment to protecting online privacy.

Finally, with regard to drafting clear, complete and understandable privacy statements, ESRB Privacy Online's services also include the provision of a team of legal and business experts who are trained to help participating companies create compliant privacy policies and statements. The team is available to work one-on-one with companies to ensure that privacy policies and statements contain collection and use practices that adhere to all of ESRB's requirements and that can meet the parameters of most existing business models.



Sentinel Oversight, Monitoring and Enforcement Services

The Sentinel Program is ESRB Privacy Online's enforcement and accountability mechanism; the apparatus that verifies that participating companies comply with their published information policies. The Sentinel Program is broken down into three distinct parts: The Sentinel Consumer Online-Hotline, Sentinel Monitoring and Verification, and Sentinel Spot Checks.

The Sentinel Consumer Online Hotline is a no-cost, online reporting system that allows consumers to easily and anonymously report possible privacy violations directly to ESRB Privacy Online.

Sentinel Monitoring and Verification is the procedure by which specially trained ESRB Privacy Online Web monitors review the information practices of a participating company, verifying constant compliance with the Principles and Guidelines. The goal of these reviews is to assure both the consumer and the participating company that a reliable safeguard exists to ensure that the company's privacy policy implementation is accurate, meaningful and effective.

Ensuring this effectiveness is also the purpose of the Sentinel Spot Checks, which consist of periodic, randomly scheduled reviews of a participating company's Web site. Spot Checks involve unannounced audits of a company's information practices by "seeding" fictitious information and tracking the results. The Sentinel Program as a whole works hand-in-hand with our alternative dispute resolution services, together offering truly efficient recourse for consumer concerns.

Alternative Dispute Resolution Services

The ESRB Privacy Online Program also provides free alternative dispute resolution ("ADR") services to assist in resolving consumer complaints that cannot be adequately addressed by the company itself. These services include mediation and arbitration administered by an ESRB Privacy Online certified ADR Officer.

The ESRB Privacy Online Program also requires participating companies to create and implement an internal dispute resolution system. This process must be designed to fairly and expeditiously resolve privacy related issues and complaints raised by either consumers or ESRB Privacy Online monitors. In addition, the ESRB Privacy Program requires participating companies to submit to the above described ESRB mediation or arbitration of consumer grievances when issues are not effectively addressed through a company's own internal mechanisms. In some instances, ESRB Privacy Online, through its ADR Officer, may also play an intermediary role as a neutral evaluator between the consumer and the participating company.



I(B) – Full text of the ESRB Privacy Online Principles and Guidelines for Fair Information Practices.

ESRB Privacy Online provides these principles and guidelines regarding the online protection of personal data for companies that participate in the ESRB Privacy Online Program. These principles and guidelines serve as the basis upon which participating companies build their own data protection policies.

1. Notice/Disclosure

Principle: Each participating company must implement and publish a “Privacy Statement” that informs consumers about its information practices.

Implementation of Notice/Disclosure Principle:

This Privacy Statement must be written in a clear and understandable manner and must state: (1) what personal identifying information may be collected, and by what means (e.g., directly or passively); (2) who is collecting the data; (3) how the information may be used, including those outside the company with whom it may be shared; (4) a statement of the organization’s commitment to data security; (5) what choices are offered the consumer to customize collection and use of their information; (6) what opportunities are offered for consumers to access their personal identifying information; (7) how consumers can ask questions or file complaints; (8) what steps the organization takes to ensure data quality; and, (9) the consequences, if any, of an individual’s refusal to provide information.

Privacy statements must be complete and must not contain any unrelated, confusing, or contradictory information.

Participating companies are required to provide a hypertext link on the first page of their Web site and at any point on their Web site where personal data is requested.¹

¹At times, these guidelines distinguish between two classes of personal data, personal identifying information and demographic data. Personal identifying information, which includes name, e-mail address, phone number, home address, social security number, driver’s license number, date of birth, etc., deserves a higher level of protection because it enables direct contact with the data subject and because the data subject has a greater interest in controlling this information. Demographic data, which may include age, gender, geographic area, hobbies, interests, and favorites, only require protection if they can be linked to an identifiable individual.

E B

Participating companies should teach consumers to make informed choices about how they allow their personal data to be used as they participate in the electronic marketplace. Participating companies may perform this consumer education themselves, through the trade association, or industry public service campaigns, or through ESRB's Privacy Online Program educational services.

2. Choice

Principle: Participating companies must give consumers the choice to exercise reasonable control over the collection and use of their personal data.

Implementation of Choice Principle:

Consumers must be provided with simple, easily understood and readily available mechanisms to exercise choice over the collection and use of their personal data. Such mechanisms may include opt-in, opt-out, or other equally effective approaches. An opt-in mechanism requires a participating company to obtain authorization from the consumer before collecting personal data from that consumer, or before using it in a particular manner. An opt-out mechanism offers the consumer an opportunity to control certain uses of personal data collected by a participating company.

The scope of choice that is reasonable, and the mechanism that is appropriate, may vary according to the sensitivity of the data, whether the data is collected from a child², the necessity of the collection or use of personal data for completing a transaction initiated by the consumer, whether the use contemplated for the data is a secondary use³ or third party distribution, the burden created by offering choice, the requirements of state or other applicable law, and other factors.

² Where a participating company wishes to collect or use the personal data of a child, the company must provide a reasonable mechanism for parents of the child to consent to the collection and use of their child's personal data or consent to the collection and use of their child's personal data without consenting to the disclosure of that data to third parties, or refuse to permit further collection or use of their child's data.

³ Secondary use is use for purposes not directly related to the purpose for which the information was collected.



3. Limiting Data Collection and Retention

Principle: Participating companies must limit the collection and retention of personal data to that which is needed for valid business reasons, and any such data must be obtained by lawful and fair means.

Implementation of Limitation Principle:

Even if a participating company has a valid business reason to collect personal data from a consumer, it must only collect that data which is needed for the valid business reason. Where the consumer is a child, a participating company must only collect that data, which is needed for the valid business, and such collection and use must be relevant to the Web site activity.

Participating companies must periodically reevaluate whether a valid business reason continues to exist for collection or retention of certain personal data, and if the valid business reason ceases to exist or ceases to require the collection or retention of certain personal data, participating companies must limit their data collection and retention practices accordingly.

4. Data Integrity/Security

Principle: Participating companies creating, maintaining, using or disseminating records of personal identifying information must take reasonable measures to assure its reliability and should take reasonable precautions to protect it from loss, misuse, or alteration.

Implementation of Data Integrity/Security Principle:

Reliable data means data that is accurate, complete, and timely. Reasonable measures to assure the reliability of personal identifying information may include, among other things, using only reputable sources of data, cross-referencing data against multiple sources, providing consumer access to data for purposes of verification and correction, and destroying untimely data or converting it to anonymous form.

Reasonable precautions to protect data may include, among other things, limiting access to such data to those employees performing a legitimate business function; technical security measures, such as encryption or passwords, to prevent unauthorized access; and the storage of data on secure servers or computers inaccessible by modem.



Participating companies must take reasonable steps to assure that third parties to whom they transfer such information are aware of these security practices, and that the third parties also take reasonable precautions to protect transferred information participating companies must obtain information, including name, address, tax identification number, telephone number and samples of material to be distributed, from third parties that buy, rent, or purchase personal data from the participating company. Because participating companies cannot always control the activities of third parties, participating companies must notify consumers that they cannot guarantee that third parties will adhere to the same security standards.

5. Data Access

Principle: Consumers must have the opportunity for reasonable, appropriate access to personal identifying information about them that a participating company holds, and must be able to correct, amend, or request the removal of that information when necessary.

Implementation of Access Principle:

When consumers are offered the opportunity to access the personal identifying information a participating company holds about them, such access must be meaningful. To be meaningful, access must encompass timely and inexpensive access to data, a simple means for contesting inaccurate or incomplete data, a mechanism by which the data collector can verify the information, the means by which corrections and/or consumer objections can be added to the data file and sent to all data recipients, and the ability of a consumer to request the removal of their personal identifying information from the data file.

The reasonableness and appropriateness of access and correction will depend on a variety of factors. These factors include the burden (e.g., cost) that providing access will place on a participating company; the nature of the information collected, including whether it is stored online or offline; the number of locations in which it is stored; the nature of the enterprise; the ways in which the information is to be used; preservation of information security; and whether the data is collected from a child.

If a participating company collects data from a child, the company must provide the parents of that child with the opportunity to review, correct and/or have deleted any and all information (e.g., personal and demographic information) collected from the child, and to refuse to permit further collection or use of the child's information.



6. Enforcement/Accountability

Principle: Participating companies must implement effective and affordable mechanisms that ensure compliance with their information privacy policies and provide appropriate means of recourse for consumers.

Implementation of Enforcement:

Participating companies must create and implement internal processes for ensuring that they comply with the privacy practices they have adopted. Participating companies must train personnel in a position to collect data from or about consumers to adhere to the stated privacy practices. Participating companies must assign specific personnel the responsibility for monitoring compliance with privacy practices participating companies must create a system of incentives and/or sanctions to encourage adherence to privacy policies.

Participating companies must also provide verification that the assertions they make about their privacy practices are true and that privacy practices have been implemented as represented. The nature and the extent of verification depends upon the kind of personal data with which a company deals -- companies collecting and using highly sensitive data may be held to a higher standard of verification.⁴ To this end, all participating companies must on a regular basis review their record of compliance with privacy practices. However, where the data collected and used is highly sensitive, verification may necessitate that the participating company hire an outside auditor to review the compliance record.

Each participating company must also create and implement internal processes affording consumers appropriate means of recourse for claimed failures by that participating company to adhere to its stated privacy practices. Appropriate means of recourse include, at a minimum, institutional mechanisms to ensure that consumers have a simple, effective way to have their concerns addressed. For example, a participating company must appoint identifiable, accessible, and responsive personnel to whom consumers can initially bring a grievance. Such personnel must be given the authority to investigate the grievance and complete this investigation in a timely manner. Such personnel must be required to submit a written response to the aggrieved consumer that details the results of the investigation, and should be given incentives to respond to consumers in a timely manner. If the participating company has not adhered to its privacy

⁴ In this instance, the sensitivity of the data derives from the nature of the data in addition to whether it can be tied to an identifiable person. For example, credit card information or other financial information that can be tied to an individual would be considered highly sensitive, while that individual's name and address without any accompanying information would be considered less sensitive.



practices, consumers must be offered a remedy for the violation. Such a remedy must be appropriate under the circumstances of the case and may include the righting of the wrong (e.g. correction of any misinformation, cessation of further data collection from that consumer, or destruction of improperly collected data) or compensation for any harm caused.

If the consumer is not satisfied with the resolution, participating companies must provide consumers with a mechanism to appeal initial decisions to higher management levels. Lastly, if the consumer is still unsatisfied regarding the resolution of a grievance, the consumer must be referred to ESRB Privacy Online's Alternative Dispute Resolution Officer.

7. Children

(a) Children Twelve and Under. With regard to the online collection of personal identifying information from children 12 and under⁵, participating companies must comply with the requirements contained in §§ 312.2 – 312.9 of the Final Rule (16 C.F.R. Part 312) implementing the Children's Online Privacy Protection Act (15 U.S.C. 6501 et seq.), including the adoption and adherence to the following guidelines:

- (1) a participating company must provide a clear and understandably written privacy statement of its privacy policies with regard to children that is complete and contains no unrelated, confusing, or contradictory materials. This privacy statement must include notice of what information it collects from children, how it uses such information, and its disclosure practices for such information. This notice must be prominent and readily accessible to all Web users, including parents and children;
- (2) a participating company must obtain verifiable parental consent prior to any collection, use, and/or disclosure of personal information from children, including consent to any material change in the collection, use, and/or disclosure practices to which

⁵ It is often difficult to determine the age of a Web site visitor. In adopting these Principles and Guidelines for children, ESRB Privacy Online recommends that participating companies operating Web sites or online services directed to children assume their visitors are twelve or under, unless they have actual knowledge that the visitor is older. Participating companies operating Web sites or online services appealing mainly to adults may, on the other hand, assume their visitors are adult, unless they have actual knowledge that a visitor is a child. Participating companies operating "mixed appeal" Web sites, which are designed to appeal to both adults and children, should ask the age of the visitor and then apply the appropriate data collection and use practices. Though requests that Web visitors identify their own age may, in certain cases, not yield totally accurate results, participating companies may rely on the age given.



the parent has previously consented. For example, where a participating company wishes to collect personal identifying information that would enable someone to contact a child offline or where a participating company wishes to post or disclose personal identifying information to third parties, the company must obtain prior verifiable parental consent⁶ (opt-in);

- (3) a participating company must provide a reasonable means for a parent to review the personal identifying information collected from a child and refuse to permit its further use or maintenance;
- (4) a participating company must 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;
- (5) a participating company must establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children; and,
- (6) each time a participating company communicates with a child by e-mail, the participating company must provide an easily activated mechanism that the child can activate to prevent the forwarding/receipt of future e-mails.

(b) Children Over Twelve and Under Eighteen. If participating companies engage in collection of personal identifying information from children over twelve and under eighteen years of age, ESRB Privacy Online recommends that participating companies provide parents with *notice*⁷ of the collection of such information and an opportunity to remove the information from the site's database (opt-out).

⁶ Mechanisms to obtain actual or 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. Acceptable mechanisms for obtaining actual or verifiable parental consent include providing a consent form to be signed by the parent and returned to the participating company by mail or fax; requiring a parent to use a credit card in connection with a transaction; having a parent call a toll-free telephone number staffed by trained personnel; using a electronic (digital) signature; and/or using e-mail accompanied by a PIN or password obtained through one of the verification methods described above. Though none of these mechanisms for securing parental consent are foolproof, they provide sufficiently high assurance that consent has been provided by the parent.

⁷ A participating company should provide notice in a manner that is likely to be effective. Notice by e-mail will be considered effective unless the participating company has reason to believe otherwise.

11

12

SECTION II

SECTION II - PROVISION COMPARISON CHART. COMPARATIVE ANALYSIS OF EACH PROVISION OF §§312.3 THROUGH 312.8 WITH THE CORRESPONDING PROVISIONS OF THE ESRB PRIVACY ONLINE PRINCIPLES AND GUIDELINES.

Section Number	Children's Online Privacy Protection Rule	Corresponding Section of ESRB Privacy Online Principles and Guidelines for Fair Information Practices
§ 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.	<p>7. Children</p> <p>(a) Children Twelve and Under. With regard to the online collection of personal identifying information from children 12 and under¹, participating companies must comply with the requirements contained in §§ 312.2 – 312.9 of the Final Rule (16 C.F.R. Part 312) implementing the Children's Online Privacy Protection Act (15 U.S.C. 6501 et seq.), including the adoption and adherence to the following guidelines:</p> <p>(1) <i>a participating company must provide a clear and understandably written privacy statement of its privacy policies with regard to children that is complete and contains no unrelated, confusing, or contradictory materials. This privacy statement must include notice of what information it collects from children, how it uses such information, and its disclosure practices for such information. This notice must be prominent and readily accessible to all Web users, including parents and children.</i></p> <p>(2) <i>a participating company must obtain verifiable parental consent prior to any collection, use, and/or disclosure of personal information from children, including consent to any material change in the collection, use, and/or disclosure practices to which the parent has previously consented. For example, where a participating</i></p>

¹ It is often difficult to determine the age of a Web site visitor. In adopting these Principles and Guidelines for children, ESRB Privacy Online recommends that participating companies operating Web sites or online services directed to children assume their visitors are twelve or under, unless they have actual knowledge that the visitor is older. Participating companies operating Web sites or online services appealing mainly to adults may, on the other hand, assume their visitors are adult, unless they have actual knowledge that a visitor is a child. Participating companies operating "mixed appeal" Web sites, which are designed to appeal to both adults and children, should ask the age of the visitor and then apply the appropriate data collection and use practices. Though requests that Web visitors identify their own age may, in certain cases, not yield totally accurate results, participating companies may rely on the age given.

company wishes to collect personal identifying information that would enable someone to contact a child offline or where a participating company wishes to post or disclose personal identifying information to third parties, the company must obtain prior parental consent²¹ (opt-in);

- (3) a participating company must provide a reasonable means for a parent to review the personal identifying information collected from a child and refuse to permit its further use or maintenance;*
- (4) a participating company must 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;*
- (5) a participating company must establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children; and,*
- (6) each time a participating company communicates with a child by e-mail, the participating company must provide an easily activated mechanism that the child can activate to prevent the forwarding/receipt of future e-mails.*

² Mechanisms to obtain actual or 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. Acceptable mechanisms for obtaining actual or verifiable parental consent include providing a consent form to be signed by the parent and returned to the participating company by mail or fax; requiring a parent to use a credit card in connection with a transaction; having a parent call a toll-free telephone number staffed by trained personnel; using a electronic (digital) signature; and/or using e-mail accompanied by a PIN or password obtained through one of the verification methods described above. Though none of these mechanisms for securing parental consent are foolproof, they provide sufficiently high assurance that consent has been provided by the parent.

See Children § (7)(a), above;

and

1. Notice/Disclosure

Principle: Each participating company must implement and publish a "Privacy Statement" that informs consumers about its information practices.

Implementation of Notice/Disclosure Principle:

This Privacy Statement must be written in a clear and understandable manner and must state: (1) what personal identifying information may be collected, and by what means (e.g., directly or passively); (2) who is collecting the data; (3) how the information may be used, including those outside the company with whom it may be shared; (4) a statement of the organization's commitment to data security; (5) what choices are offered the consumer to customize collection and use of their information; (6) what opportunities are offered for consumers to access their personal identifying information; (7) how consumers can ask questions or file complaints; (8) what steps the organization takes to ensure data quality; and, (9) the consequences, if any, of an individual's refusal to provide information.

Privacy statements must be complete and must not contain any unrelated, confusing, or contradictory information.

Participating companies are required to provide a hypertext link on the first page of their Web site and at any point on their Web site where personal data is requested.³

Participating companies should teach consumers to make informed choices about how they allow their personal data to be used as they participate in the electronic marketplace.

³ At times, these guidelines distinguish between two classes of personal data, personal identifying information and demographic data. Personal identifying information, which includes name, e-mail address, phone number, home address, social security number, driver's license number, date of birth, etc., deserves a higher level of protection because it enables direct contact with the data subject and because the data subject has a greater interest in controlling this information. Demographic data, which may include age, gender, geographic area, hobbies, interests, and favorites, only require protection if they can be linked to an identifiable individual.

§ 312.5	Parental consent.	Participating companies may perform this consumer education themselves, through the trade association, or industry public service campaigns, or through ESRB's Privacy Online Program educational services.
		<p>See <i>Children</i> §§ (7)(a) - (a)(2)(iii), above;</p> <p style="text-align: center;"><i>and</i></p> <p>2. Choice</p> <p>Principle: Participating companies must give consumers the choice to exercise reasonable control over the collection and use of their personal data.</p> <p><i>Implementation of Choice Principle:</i></p> <p><i>Consumers must be provided with simple, easily understood and readily available mechanisms to exercise choice over the collection and use of their personal data. Such mechanisms may include opt-in, opt-out, or other equally effective approaches. An opt-in mechanism requires a participating company to obtain authorization from the consumer before collecting personal data from that consumer, or before using it in a particular manner. An opt-out mechanism offers the consumer an opportunity to control certain uses of personal data collected by a participating company.</i></p> <p><i>The scope of choice that is reasonable, and the mechanism that is appropriate, may vary according to the sensitivity of the data, whether the data is collected from a child⁴, the necessity of the collection or use of personal data for completing a transaction initiated by the consumer, whether the use contemplated for the data is a secondary use⁵ or third party distribution, the burden created by offering choice, the requirements of state or other applicable law, and other factors.</i></p>

⁴ Where a participating company wishes to collect or use the personal data of a child, the company must provide a reasonable mechanism for parents of the child to consent to the collection and use of their child's personal data or consent to the collection and use of their child's personal data without consenting to the disclosure of that data to third parties, or refuse to permit further collection or use of their child's data.

⁵ Secondary use is use for purposes not directly related to the purpose for which the information was collected.

Right of parent to review personal information provided by a child.

See *Children §§ 7(a) and 7(a)(3)*, above;

and

4. Data Integrity/Security

Principle: Participating companies creating, maintaining, using or disseminating records of personal identifying information must take reasonable measures to assure its reliability and should take reasonable precautions to protect it from loss, misuse, or alteration.

Implementation of Data Integrity/Security Principle:

Reliable data means data that is accurate, complete, and timely. Reasonable measures to assure the reliability of personal identifying information may include, among other things, using only reputable sources of data, cross-referencing data against multiple sources, providing consumer access to data for purposes of verification and correction, and destroying untimely data or converting it to anonymous form.

Reasonable precautions to protect data may include, among other things, limiting access to such data to those employees performing a legitimate business function; technical security measures, such as encryption or passwords, to prevent unauthorized access; and the storage of data on secure servers or computers inaccessible by modem.

Participating companies must take reasonable steps to assure that third parties to whom they transfer such information are aware of these security practices, and that the third parties also take reasonable precautions to protect transferred information participating companies must obtain information, including name, address, tax identification number, telephone number and samples of material to be distributed, from third parties that buy, rent, or purchase personal data from the participating company. Because participating companies cannot always control the activities of third parties, participating companies must notify consumers that they cannot guarantee that third parties will adhere to the same security standards.

<p>§ 312.7</p> <p>Prohibition against conditioning a child's participation on collection of personal information.</p>	<p><i>See Children §§ 7(a) and (7)(a)(4), above;</i> <i>and</i></p> <p>3. Limiting Data Collection and Retention</p> <p>Principle: Participating companies must limit the collection and retention of personal data to that which is needed for valid business reasons, and any such data must be obtained by lawful and fair means.</p> <p><i>Implementation of Limitation Principle:</i></p> <p><i>Even if a participating company has a valid business reason to collect personal data from a consumer, it must only collect that data which is needed for the valid business reason. Where the consumer is a child, a participating company must only collect that data which is needed for the valid business and such collection and use must be relevant to the website activity. Participating companies must periodically reevaluate whether a valid business reason continues to exist for collection or retention of certain personal data, and if the valid business reason ceases to exist or ceases to require the collection or retention of certain personal data, participating companies must limit their data collection and retention practices accordingly.</i></p>
<p>§ 312.8</p> <p>Confidentiality, security, and integrity of personal information collected from children.</p>	<p><i>See Children §§ 7(a), (7)(a)(5), above;</i> <i>and</i></p> <p>4. Data Integrity/Security</p> <p>Principle: Participating companies creating, maintaining, using or disseminating records of personal identifying information must take reasonable measures to assure its reliability and should take reasonable precautions to protect it from loss, misuse, or alteration.</p>

Implementation of Data Integrity/Security Principle:

Reliable data means data that is accurate, complete, and timely. Reasonable measures to assure the reliability of personal identifying information may include, among other things, using only reputable sources of data, cross-referencing data against multiple sources, providing consumer access to data for purposes of verification and correction, and destroying untimely data or converting it to anonymous form.

Reasonable precautions to protect data may include, among other things, limiting access to such data to those employees performing a legitimate business function; technical security measures, such as encryption or passwords, to prevent unauthorized access; and the storage of data on secure servers or computers inaccessible by modem.

Participating companies must take reasonable steps to assure that third parties to whom they transfer such information are aware of these security practices, and that the third parties also take reasonable precautions to protect transferred information participating companies must obtain information, including name, address, tax identification number, telephone number and samples of material to be distributed, from third parties that buy, rent, or purchase personal data from the participating company. Because participating companies cannot always control the activities of third parties, participating companies must notify consumers that they cannot guarantee that third parties will adhere to the same security standards.

E

B

SECTION III



SECTION III – STATEMENT EXPLAINING: (i) HOW ESRB PRIVACY ONLINE PROGRAM REQUIREMENTS, PRINCIPLES AND GUIDELINES FOR FAIR INFORMATION PRACTICES, AND APPLICABLE ASSESSMENT MECHANISMS MEET THE REQUIREMENTS OF THE FINAL RULE; AND, (ii) HOW THE ASSESSMENT MECHANISM AND COMPLIANCE INCENTIVES MEET THE REQUIREMENTS OF THE FINAL RULE.

III(A) - How ESRB Privacy Online Program requirements, Principles and Guidelines for Fair Information Practices, and Applicable Assessment Mechanisms Meet the Requirements of the Final Rule.

ESRB Privacy Online Principles and Guidelines and applicable assessment mechanisms meet and exceed the requirements of the Final Rule as requested in §312.10. The Principles and Guidelines themselves were drafted based on Federal Trade Commission endorsed Fair Information Practices, the Children’s Online Privacy Protection Act, and the specific requirements set forth under the Final Rule. Each provision contained in §§312.2 through 312.9 of the Final Rule can be matched with a corresponding provision within the ESRB Privacy Online Principles and Guidelines (*Please see Provision Comparison Chart, Section II, herein*). The scope and substance of the Principles and Guidelines were drafted to encompass the same, or substantially similar, criteria delineated in the Final Rule and in generally accepted online fair information practices. As a result, participating companies that follow our privacy program are required to implement policies and procedures that provide the same—and in many cases greater—protections for children and all Web users as those contained in the Final Rule. For example:

Defined Terms. With regard to §312.2, in addition to the existing defined terms found in the ESRB Privacy Online license agreement, the definitions of each term set forth in §312.2 of the Final Rule are also contained in the Agreement. As a result, all participating companies are required to interpret these terms in a manner consistent with the definitions of §312.2.

General Requirements. Under §312.3, the Final Rule sets forth five (5) general criteria to ensure that no operator of a Web site or online service directed to children, or any operator that has actual knowledge that it is collecting or maintaining personal information from a child, collect this personal information in a manner that violates the Final Rule. Specifically, §312.3 states that an operator must:

- (1) post a privacy statement on their Web site of what information the company collects from children, how the company uses such information, and the company’s disclosure practices for such information;



- (2) obtain verifiable parental consent prior to any collection, use, and/or disclosure of personal information from children;
- (3) 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;
- (4) 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,
- (5) establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.

Under our program requirements and Principles and Guidelines, ESRB Privacy Online requires that these exact same standards be met. In addition, ESRB Privacy Online also requires, generally, that all participating companies comply with the following Principles:

- **Notice/Disclosure** - each participating company must implement and publish a complete "Privacy Statement" that informs consumers, in a clear and understandably written manner, about *all* its information practices;
- **Choice** - participating companies must give consumers the choice to exercise reasonable control over the collection and use of their personal data;
- **Limiting Data Collection and Retention** – participating companies must limit the collection and retention of personal data to that which is needed for valid business reasons, and any such data must be obtained by lawful and fair means;
- **Data Integrity/Security** - participating companies creating, maintaining, using or disseminating records of personal identifying information must take reasonable measures to assure its reliability and must take reasonable precautions to protect it from loss, misuse, or alteration;
- **Data Access** - consumers must have the opportunity for reasonable, appropriate access to personal identifying information about them that a participating company holds, and must be able to correct, amend, or request the removal of that information when necessary;
- **Enforcement/Accountability** - participating companies must implement effective and affordable mechanisms that ensure compliance with their information privacy policies and provide appropriate means of recourse for consumers; and,



- **Children** – participating companies must comply with the requirements contained in §§ 312.2 – 312.9 of the Final Rule (16 C.F.R. Part 312) implementing the Children’s Online Privacy Protection Act (15 U.S.C. 6501 et seq.).

As the Principles and Guidelines demonstrate (*Please see Section I(B), Principles and Guidelines, herein*), the implementation of the Principles results in a more comprehensive scope than summarized above, including strict requirements regarding standards, implementation and the general administration of the Principles with regard to a company’s information collection practices. In total, these Principles and Guidelines meet and exceed the requirements set forth in §312.10. For example:

Notice. With regard to Notice, the ESRB Privacy Online Program meets the Final Rule’s requirements by setting forth the same criteria as described in §312.4. In addition to these requirements, the Principles and Guidelines require that participating companies publish a privacy statement that states: (1) what personal identifying information may be collected, and by what means (e.g., directly or passively); (2) who is collecting the data; (3) how the information may be used, including those outside the company with whom it may be shared; (4) a statement of the organization’s commitment to data security; (5) what choices are offered the consumer to customize collection and use of their information; (6) what opportunities are offered for consumers to access their personal identifying information; (7) how consumers can ask questions or file complaints; (8) what steps the organization takes to ensure data quality; and (9) the consequences, if any, of an individual’s refusal to provide information.

ESRB Privacy Online’s Notice Principle also requires that statements must be complete and must not contain any unrelated, confusing, or contradictory information. Participating companies are required to provide a hypertext link on the first page of their Web site and at any point on their Web site where personal data is requested.¹³ The ESRB Privacy Online License Agreement also contains provisions that regulate the placement, size, and operation of the link. Specifically, under §2.4, the Agreement states:

¹³At times, these guidelines distinguish between two classes of personal data, personal identifying information and demographic data. Personal identifying information, which includes name, e-mail address, phone number, home address, social security number, driver’s license number, date of birth, etc., deserves a higher level of protection because it enables direct contact with the data subject and because the data subject has a greater interest in controlling this information. Demographic data, which may include age, gender, geographic area, hobbies, interests, and favorites, only require protection if they can be linked to an identifiable individual.



2.4 The Mark

(a) At Licensee's discretion, Licensee shall display either: (i) Version 1 of the Mark ("click-to-Privacy Statement" seal, see Exhibit A); or, (ii) an alternative graphic supplied by ESRB Privacy Online ("alternative graphic"), on the first page of its Web Site, Main Pages of its Web Site as defined and designated by ESRB Privacy Online, and any other page within Licensee's Web Site where a User is requested to provide Personal Identifying Information. Such placement shall be in a location, format, and manner selected by Licensee in its reasonable discretion and reasonably approved by ESRB Privacy Online. Licensee shall not alter or cause or authorize the alteration of the Mark or of the alternative graphic in any manner whatsoever without the express prior written permission of ESRB Privacy Online and shall match the size of the Mark displayed upon Licensee's Web Site with the Mark on Exhibit A, or, in the event Licensee displays the alternative graphic, then, Licensee shall match the size of such alternative graphic to the exact dimensions specified by ESRB Privacy Online, which dimensions shall in any event be no larger than the Mark's dimensions. The placement of such Mark or alternative graphic shall be subject to ESRB Privacy Online's reasonable approval. Such Mark or alternative graphic shall be part of a graphical user interface and shall activate a hyperlink that shall directly access Licensee's Privacy Statement.

(b) Licensee shall display Version 2 of the Mark ("click-to-confirm" seal, see Exhibit B) on the first page of its Privacy Statement in a location, format and manner reasonably prescribed by ESRB Privacy Online. Licensee shall not alter or cause or authorize the alteration of the Mark in any manner whatsoever without the express, prior written permission of ESRB Privacy Online and shall match the size of the Mark displayed upon Licensee's Web Site with the Mark on Exhibit B. The placement of such Mark shall be subject to ESRB Privacy Online's reasonable approval. Such Mark shall be part of a graphical user interface, provided by ESRB Privacy Online, and shall activate a hyperlink that shall directly access an ESRB Privacy Online server for authentication purposes.

(c) Licensee shall provide ESRB Privacy Online, within ten (10) business days of Web Site certification by ESRB Privacy Online, with the URL(s) of the Version 1 Mark(s) or the alternative graphic and must



provide ESRB Privacy Online with five (5) business days notice, as set forth in Section 13.0, herein, prior to changing such URL(s).

(d) If Licensee engages another party to provide hosting services for Licensee's Web Site, Licensee is responsible for ensuring such party displays, as the case may be, either Version 1 and 2 of the Mark or the alternative graphic and Version 2 of the Mark as set forth in this Agreement.

Under the Notice Principle, participating companies are also required to teach consumers to make informed choices about how they allow their personal data to be used as they participate in the electronic marketplace. Participating companies may perform this consumer education themselves, through the trade association, or industry public service campaigns, or through ESRB's Privacy Online Program educational services.

Parental Consent. With regard to parental consent requirements, the ESRB Privacy Online Program also meets and exceeds the requirements in the Final Rule. Participating companies must comply with the requirements contained in §312.5 by obtaining verifiable parental consent prior to any collection, use, and/or disclosure of personal information from children, including consent to any material change in the collection, use, and/or disclosure practices to which the parent has previously consented. Mechanisms to obtain actual or 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. Acceptable mechanisms for obtaining actual or verifiable parental consent include providing a consent form to be signed by the parent and returned to the participating company by mail or fax; requiring a parent to use a credit card in connection with a transaction; having a parent call a toll-free telephone number staffed by trained personnel; using a electronic (digital) signature; and/or using e-mail accompanied by a PIN or password obtained through one of the verification methods described above. Though none of these mechanisms for securing parental consent are foolproof, they provide sufficiently high assurance that consent has been provided by the parent.

ESRB Privacy Online exceeds the requirements in §312.5 by requiring that participating companies give all consumers the choice to exercise reasonable control over the collection and use of their personal data. Consumers must be provided with simple, easily understood and readily available mechanisms to exercise choice over the collection and use of their personal data. Mechanisms may include opt-in, opt-out, or other equally effective approaches. An opt-in mechanism requires participating company to obtain authorization from the consumer before collecting personal data from that consumer, or before using it in a particular manner. An opt-out mechanism offers the consumer an opportunity to control certain uses of personal data collected by a participating company.



The scope of choice that is reasonable, and the mechanism that is appropriate, may vary according to the sensitivity of the data, whether the data is collected from a child¹⁴, the necessity of the collection or use of personal data for completing a transaction initiated by the consumer, whether the use contemplated for the data is a secondary use or third party distribution, the burden created by offering choice, the requirements of state or other applicable law, and other relevant factors.

Right of Parent to Review Personal Information Provided by a Child. In addition to requiring that the same criteria be met as contained in §312.6, ESRB Privacy Online also requires that all consumers have the opportunity for reasonable, appropriate access to personal identifying information about them that a participating company holds, and must be able to correct or amend that information when necessary. As stated in the Principles and Guidelines (*Please see Principles and Guidelines, Access; Section I(B), herein*), when consumers are offered the opportunity to access the personal identifying information a participating company holds about them, such access must be meaningful. To be meaningful, access must encompass timely and inexpensive access to data, a simple means for contesting inaccurate or incomplete data, a mechanism by which the data collector can verify the information, and the means by which corrections and/or consumer objections can be added to the data file and sent to all data recipients.

The reasonableness and appropriateness of access and correction will depend on a variety of factors. These factors include the burden (e.g., cost) that providing access will place on a participating company; the nature of the information collected, including whether it is stored online or offline; the number of locations in which it is stored; the nature of the enterprise; the ways in which the information is to be used; preservation of information security; and whether the data is collected from a child.

If a participating company collects data from a child, the company must provide the parents of that child with the opportunity to review, correct and/or have deleted any and all information (e.g., personal and demographic information) collected from the child, and refuse to permit further collection or use of the child's information.

¹⁴ Where a participating company wishes to collect or use the personal data of a child, the company must provide a reasonable mechanism for parents of the child to consent to the collection and use of their child's personal data or consent to the collection and use of their child's personal data without consenting to the disclosure of that data to third parties, or refuse to permit further collection or use of their child's data.



Prohibition Against Conditioning a Child's Participation on Collection of Personal

Information. ESRB Privacy Online again meets and exceeds the requirements of §312.7 by matching the criteria set forth in the Final Rule and by requiring participating companies to limit the collection and retention of personal data to that which is needed for valid business reasons, and that any such data must be obtained by lawful and fair means.

In addition, even if a participating company has a valid business reason to collect personal data from a consumer, it must only collect that data which is needed for the valid business reason. Where the consumer is a child, a participating company must only collect that data which is needed for the valid business reason and such collection and use must be relevant to the Web site activity. Participating companies must periodically reevaluate whether a valid business reason continues to exist for collection or retention of certain personal data, and if the valid business reason ceases to exist or ceases to require the collection or retention of certain personal data, participating companies must limit their data collection and retention practices accordingly.

Confidentiality, Security, and Integrity of Personal Information Collected from Children.

ESRB Privacy Online meets and exceeds the requirements in §312.8 by requiring that participating companies that create, maintain, use or disseminate records of personal identifying information must also take reasonable measures to assure its reliability and take reasonable precautions to protect it from loss, misuse, or alteration.

Reliable data means data that is accurate, complete, and timely. Reasonable measures to assure the reliability of personal identifying information may include, among other things, using only reputable sources of data, cross-referencing data against multiple sources, providing consumer access to data for purposes of verification and correction, and destroying untimely data or converting it to anonymous form.

Reasonable precautions to protect data may include, among other things, limiting access to such data to those employees performing a legitimate business function; technical security measures, such as encryption or passwords, to prevent unauthorized access; and the storage of data on secure servers or computers inaccessible by modem.

Participating companies must take reasonable steps to assure that third parties to whom they transfer such information are aware of these security practices, and that the third parties also take reasonable precautions to protect transferred information. Participating companies must obtain information, including name, address, tax identification number, telephone number and samples of material to be distributed, from third parties that buy, rent, or purchase personal data



from the participating company. Because participating companies cannot always control the activities of third parties, participating companies must notify consumers that they cannot guarantee that third parties will adhere to the same security standards.

Assessment Mechanisms. ESRB Privacy Online assessment mechanisms also meet and exceed the requirements of the Final Rule. Participating companies are required to create and implement internal processes for ensuring that they comply with the privacy practices they have adopted. Participating companies are also required to train personnel in a position to collect data from or about consumers to adhere to the stated privacy practices. Participating companies assign specific personnel the responsibility for monitoring compliance with privacy practices and are also strongly encouraged to create a system of incentives and/or sanctions to encourage adherence to privacy policies.

Participating companies are also required to provide verification that the assertions they make about their privacy practices are true and that privacy practices have been implemented as represented. The nature and the extent of verification depends upon the kind of personal data with which a company deals—companies collecting and using highly sensitive data may be held to a higher standard of verification. To this end, all participating companies are required to review their record of compliance with privacy practices. However, where the data collected and used is highly sensitive, verification may necessitate that the participating company hire an outside auditor to review the compliance record.

Each participating company is also required to create and implement internal processes that afford consumers appropriate means of recourse for claimed failures by that participating company to adhere to its stated privacy practices. Appropriate means of recourse include, at a minimum, institutional mechanisms to ensure that consumers have a simple, effective way to have their concerns addressed. For example, a participating company is required to appoint identifiable, accessible, and responsive personnel to whom consumers can initially bring a grievance. Such personnel must be given the authority to investigate the grievance and complete this investigation in a timely manner. Such personnel are required to submit a written response to the aggrieved consumer that details the results of the investigation, and should be given incentives to respond to consumers in a timely manner. If the participating company has not adhered to its privacy practices, consumers must be offered a remedy for the violation. Such a remedy should be appropriate under the circumstances of the case and may include the righting of the wrong (e.g. correction of any misinformation, cessation of further data collection from that consumer, or destruction of improperly collected data) or compensation for any harm caused.

If the consumer is not satisfied with the resolution, participating companies are required to provide consumers with a mechanism to appeal initial decisions to higher management levels. Lastly, if the consumer is still unsatisfied regarding the resolution of a grievance, the



participating company is required to refer the consumer to ESRB Privacy Online's Alternative Dispute Resolution Officer.

In addition to these internal assessment mechanisms that meet the criteria set forth in the Final Rule, the ESRB Privacy Online Program exceeds the criteria stated in the Final Rule, through its own, independent enforcement and accountability mechanism: the Sentinel Program. As described above in Section I(A), the Sentinel Program is divided into three distinct parts:

The Sentinel Consumer Online-Hotline, Sentinel Monitoring and Verification, and Sentinel Spot Checks. The Sentinel Consumer Online Hotline is a no-cost, online reporting system that allows consumers to easily and anonymously report possible privacy violations directly to ESRB Privacy Online.

Sentinel Monitoring and Verification is the procedure by which specially trained ESRB Privacy Online Web Monitors randomly review the information practices of a participating company, verifying constant compliance with the Principles and Guidelines. The goal of these reviews is to assure both the consumer and the participating company that a reliable safeguard exists to ensure that the company's privacy policy implementation is meaningful and effective.

Ensuring this effectiveness is also the purpose of the Sentinel Spot Checks, which consist of periodic, randomly scheduled reviews of a participating company's Web site. Spot Checks involve unannounced audits of a participating company's information practices by "seeding" fictitious information and tracking the results. The Sentinel Program as a whole works hand-in-hand with our alternative dispute resolution services, together offering the most meaningful, effective recourse for consumer concerns available.

The Sentinel Program is discussed in more detail below in Section III(B), ESRB Privacy Online's statement of how its assessment mechanism and compliance incentives provide effective enforcement under the Final Rule.



III(B) – How the Assessment Mechanism and Compliance Incentives Required Under §312.10(b)(2) and (3) Provide Effective Enforcement of the Requirements Set Forth in the Final Rule.

Mandatory mechanism for the independent assessment of a subject operators' compliance with the guidelines. Under §312.10(b)(2), an effective, mandatory mechanism for the independent assessment of a company's compliance with the Principles and Guidelines is required. The ESRB Privacy Online Program provides a number of effective assessment mechanisms, all within the meaning of §312.10(b)(2). These assessment mechanisms are conducted through the ESRB Sentinel Program; the oversight and enforcement arm of our seal program and our tool for ensuring that participating companies comply with our program requirements. The Sentinel Program provides effective enforcement in the following ways:

Sentinel On-Site Audits. Prior to certification, and at annual intervals thereafter, each participating company must submit to an on-site audit. Each on-site audit is conducted by a staff attorney who is trained in the area of privacy law. Through these on-site audits, ESRB Privacy Online determines whether a company's privacy statement is an accurate representation of its internal and external information practices. The on-site audit also provides ESRB Privacy Online with the opportunity to ensure that a company's information practices meet all of our program's requirements and such requirements are maintained on a consistent basis. ESRB will not grant or renew a certification without first conducting an on-site audit and certifying that a company meets the program's criteria. ESRB Privacy Online maintains a record of each participating company's on-site audit for a period of three (3) years.

Sentinel Monitoring and Verification. ESRB Privacy Online also conducts both random and scheduled quarterly reviews of a participating company's information practices. The goal of these reviews is to provide effective ongoing enforcement and assure both the consumer and the participating company that a reliable safeguard exists to verify that a company's privacy policy implementation is accurate, meaningful and effective. Monitoring reviews are unannounced and consist of specially trained online monitors methodically moving through a participating company's Web site, Web page by Web page, URL by URL, ensuring that: (i) a functional link to the participating company's privacy statement is posted on its homepage, all main pages, and at all information entry points; (ii) all personal information entry points include a date of birth field that can determine if a user is twelve years old or under and then activate the information entry point to not collect personal information and instead trigger a parental consent mechanism¹⁵; and, (iii) comply with all other ESRB Privacy Online Program requirements. Each monitor is required to complete a comprehensive report that memorializes the reviewed

¹⁵ A participating company may collect the name or online contact information of a parent or child to be used for the sole purpose of obtaining parental consent. In this case, personal information cannot be used for any other purpose besides sending notice to a parent and



company's practices and must archive the site through an actual CD-ROM duplication. Both the monitor's report and the CD-ROM are maintained by ESRB Privacy Online for a period of three (3) years.

Sentinel Spot Checks. ESRB Privacy Online also periodically conducts unannounced audits of each company's privacy practices through planted "spot checks." Sentinel Spot Checks are random, unannounced reviews of a participating company's online information practices through a process known as "seeding." The seeding of a participating company's database is done by a Web monitor who submits fictitious consumer data at each information entry point. The Web site's response is then tracked and recorded to determine if the company's collection and use practices adheres to its privacy statement.

Consumer Online-Hotline. Another effective method for enforcement used by ESRB Privacy Online is the Sentinel Consumer Online-Hotline. The Sentinel Consumer Online-Hotline is a no-charge service that allows Web users who have a privacy grievance or who believe that a privacy violation has taken place on a participating company's Web site to directly report the violation/grievance to ESRB Privacy Online. The reporting can be done swiftly and easily by filling out the Sentinel Consumer Online-Hotline form and indicating on the form the alleged privacy violation. ESRB Privacy Online responds immediately to all consumer concerns and/or complaints (*See Consumer Redress below*).

Effective incentives for subject operators' compliance with the guidelines. Under §312.10(b)(3), ESRB Privacy Online must provide effective incentives for a participating company's compliance with its Principles and Guidelines. This performance standard is satisfied by ESRB Privacy Online through the following ways:

Contractual Obligations. To participate in the ESRB Privacy Online Program and post a Certification Seal, a company must first execute the ESRB Privacy Online License Agreement. As part of this Agreement and as a material obligation, participating companies must agree to comply at all times with the Principles and Guidelines. Failure to comply with any Principle and Guideline would be interpreted by ESRB Privacy Online as a material breach of the Agreement and constitute a trademark infringement and a dilution of the goodwill and reputation attaching to our mark. As a result, this contractual arrangement serves as an effective incentive for participating companies to comply with our Principles and Guidelines. In the event of such a material breach, ESRB Privacy Online is prepared to pursue a number of remedies available at law, including compensation in the form of payments to the United States Treasury.

asking for consent to collect the child's information. Such information cannot be retained for a period that exceeds thirty (30) days.



Consumer Redress. ESRB Privacy Online also requires that each participating company maintain an internal dispute resolution system that provides consumers with the ability to fairly and expeditiously resolve privacy grievances and receive appropriate remedies. Specifically, each participating company must create a simple, effective system that allows a Web user to lodge a complaint against a participating company. Each company must appoint an identifiable, accessible, and responsive individual who will serve as the participating company's privacy policy administrator. This privacy policy administrator must be given the authority to investigate a Web user's complaint and complete any necessary investigations in a timely manner. If the privacy policy administrator determines that a complaint is valid and/or that the participating company has not adhered to its information practices, the Web user should be offered a remedy. Such remedy must be appropriate under the circumstances of the case and may include the righting of the wrong (e.g., correction of any misinformation, cessation of further data collection from that consumer, or destruction of improperly collected data) or compensation for any harm caused.

If a Web user is still unsatisfied with the resolution of a complaint, or any other aspect of the participating company's internal dispute resolution process, the complaint must be directed to the ADR Officer at ESRB Privacy Online either at the Web user's own initiative or by company referral. At this point, ESRB Privacy Online, under the auspices of its ADR Officer, will implement its resolution processes, including investigations and compliance reviews. ESRB Privacy Online sponsored mediation or arbitration services seek to resolve disputes or complaints within a seven (7) to fourteen (14) day period.

Both ESRB Privacy Online and the participating company must maintain accurate records of any complaints and response to such complaints for a period of three (3) years.

Commission Referral. If a participating company fails to take appropriate actions in response to a valid complaint or an ESRB Privacy Online mandate, or in any way engages in a pattern of violating ESRB Privacy Online requirement's, ESRB Privacy Online may revoke the participating company's Certification Seal, cancel the participating company's membership status, require payments to the United States Treasury, and is prepared to refer such company to appropriate governmental authorities, as well as pursue any other remedies available at law.