ENTERTAINMENT SOFTWARE RATING BOARD
317 MADISON AVENUE 22ND FLOOR NEW YORK, NY 10017 212 759 0700 I FAX 212 759 2223
WWW.ESRB.ORG

SENT FEDERAL EXPRESS AND VIA ELECTRONIC MAIL

June 23, 2013

The Honorable Donald S. Clark
Secretary
Federal Trade Commission
Room H-172
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: Children's Online Privacy Protection Rule: Submission of Amended Safe Harbor (ESRB Privacy Certified Kids' Seal) Program Requirements – ***RESUBMISSION(Redacted Version)***

Dear Mr. Secretary:

Upon review of our earlier submission on March 1, 2013, pursuant to the revised Children's Online Privacy Protection Rule ("COPPR") announced in the Federal Register on January 17, 2013 (16 C.F.R. Part 312), the Entertainment Software Rating Board ("ESRB"), which operates the ESRB Privacy Certified (formerly ESRB Privacy Online) Program ("Program"), respectfully submits proposed changes to our Safe Harbor/Kids Seal Program Guidelines for review and approval pursuant to §312.11(e).

The following materials are attached:

Exhibit I provides (A) a brief overview of the Program; (B) specifics about the Program's oversight process; (C) statement under §312.11(c); (D) explanation of the Program's annual reporting process pursuant to §312.11(d), and; (E) a summary of additional supporting documentation.

Exhibit II: ESRB Privacy Certified Kids Seal Requirements, i.e. COPPA Safe Harbor program requirements.

Exhibits III – VII: Due to the proprietary nature and for those documents we previously submitted under separate cover that were marked "CONFIDENTIAL", the following documents, have been redacted for this part of the submission:

Exhibit III: ESRB Privacy Certified Participation Agreement.
Exhibit IV : sample compliance report.
Exhibit V: Self-Assessment Questionnaire, as referenced throughout Exhibits I-III.
Exhibit VI: Amended COPPA Rule Self-Assessment Questionnaire, the purpose of which is detailed in Exhibit I(E).
Exhibit VII**:** Amended COPPA Rule checklist, the purpose of which is detailed in Exhibit I(E).

ESRB Privacy Certified commends the FTC for its ongoing work on children's privacy. We take our designation as a "Safe Harbor" seriously and are pleased to submit these amended guidelines to the FTC . We take pride in our program and look forward to renewing our demonstrated commitment to upholding the FTC's standards and protecting the online privacy of children.

If you require any additional information, or have any questions about any of the attached materials, please do not hesitate to contact me directly at 917-522-3267.

Thank you for your consideration.

Sincerely,

Dona J. Fraser

Dona J. Fraser
Vice President, ESRB Privacy Certified

Enclosures

cc (w/ enclosures):
Patricia Vance – President, ESRB
(via email)

EXHIBIT I

(A) – Brief Overview of ESRB Privacy Online

ESRB Privacy Online is a division of the Entertainment Software Rating Board ("ESRB"), the non-profit self-regulatory body that administers the rating system for computer and video games in the U.S. and Canada, and enforces industry-adopted advertising and marketing guidelines. Established in 1994, the ESRB is the premier ratings authority for the interactive entertainment industry and has earned a reputation as a reliable and credible organization that consumers and industry members alike trust.

Building on the experience, knowledge and success of ESRB, the Privacy Online Program was launched in 1999. As one of the first programs to be approved as a COPPA Safe Harbor, ESRB Privacy Online has become the seal of choice among interactive entertainment publishers, devoted to helping our members comply with the growing complexity of privacy protection laws in the U.S. and abroad, while striving to make their websites, mobile apps and online services secure, reliable and private places to share information and conduct business. From its inception, Privacy Online has been consistently providing member companies with "privacy by design" solutions, understanding that no two companies have the same data collection practices and no two websites, apps or online services are the same.

As of April 1, 2013 ESRB Privacy Online will officially be re-branded as ESRB Privacy Certified ("EPC"). At this time, a mobile privacy seal program will also be launched. (For the avoidance of any doubt, the Kids' Seal Program Guidelines presented here shall be incorporated into the forthcoming mobile privacy seal program requirements.)

EPC will continue to maintain its high standards of compliance by:

- Providing up-front assessments of companies' products (i.e. websites, mobile apps), which begin with companies completing our detailed and thorough Self-Assessment Questionnaire;
- Reviewing existing privacy policies, terms of use and/or end-user license agreements. In addition to assisting in the drafting of privacy policies, EPC reconciles all policies and agreements (EULAs, TOS', contest rules, etc.) with applicable privacy policies to ensure consistency in the company's data collection, use, retention and sharing practices;
- Consistently monitoring and seeding products;
- Providing regular monitoring reports, which outline any required changes that may be necessary to remain in compliance with EPC's program requirements as well as best practices recommendations in the areas of behavioral advertising, data security/breach, social networking, global compliance, et al;
- Ongoing consultation services: as companies effectuate changes to their data collection practices, EPC's availability to member companies ensures ongoing compliance with EPC program requirements and industry best practices and standards;
- Vetting member companies' third parties and their data collection practices thereby assuring that member companies are partnering with companies that are upholding the same high standards of compliance;
- Providing dispute resolution services for member companies; and
- Visiting member companies for onsite audits.

(B) – Specifics about ESRB Privacy Certified's Oversight Process

For companies that seek to participate in ESRB Privacy Certified's program, EPC will conduct a thorough, comprehensive, free risk assessment of any existing products (e.g. website, mobile app). This no-obligation review provides the company with a "grade report" summarizing their existing compliance issues and existing liabilities, if any, as they pertain to U.S. and global privacy laws and best practices. A risk assessment can be provided at the initial development stages by providing EPC with wireframes or product planning summaries.

Upon completion of the more detailed Self-Assessment Questionnaire, and depending upon where the company is in its development stages, EPC works closely with the company to ensure their privacy practices are compliant, which will ensure their ability to ultimately place our seals on their sites and/or apps which shall signify to consumers, regulators and the like that they, as a company, have voluntarily taken the necessary steps to ensure the privacy and security of their users' personal information.

In addition to the bi-annual compliance reports provided to all member companies (as outlined in the attached program requirements), throughout the year and between reporting periods, members' websites and apps are routinely monitored and seeded. This is to ensure that the company's actual data collection practices remain consistent with what is stated in their privacy policies and other user agreements.

Member companies are required to submit new websites, apps and/or online services to EPC for review prior to making them available to the public so that we can, once again, ensure compliance with their stated data collection practices, as well as general compliance with applicable laws and best practices. In addition, member companies are required to notify EPC of any material changes to their data collection practices prior to implementing them with their users. If these material changes require an update to the member company's privacy policies or other user agreements, EPC will provide such updates.

The attached program requirements (Exhibit III) provide additional detailed information about the continuing obligations of our member companies, including how EPC address consumer complaints and our Dispute Resolution process.

(C) -- Statement under §312.11(c) – Request for Commission approval of self-regulatory guidelines

In accordance with the relevant provisions of §312.11(c), ESRB Privacy Certified hereby submits the following:

(1) *ESRB Privacy Certified Participation Agreement (Exhibit III – marked "CONFIDENTIAL").* This document, along with its accompanying schedules, shall provide the Commission with a detailed explanation of EPC's business model and processes as requested under §312.11(c)(1), as well as §312.11(c)(4)(i) (specifically, how the self-regulatory program guidelines meet the requirements stated under §312.11(c)). Member companies are obligated to execute this participation agreement which serves as an effective incentive for them to maintain compliance with the program's requirements. This agreement includes referenced schedules A-F, addressing other specific program requirements (e.g. EU), trademarks ("seals") and accompanying fee schedule (all marked "CONFIDENTIAL".)

(2) *ESRB Privacy Certified Kids Seal Requirements (Exhibit II).* For ease of reference, the changes to EPC's existing guidelines have been highlighted in yellow. We submit that this portion of our application fulfills the requirements of §312.11(c)(2) (i.e. a copy of the full text of the guidelines), §312.11(c)(3) (i.e. a comparison of each provision of §312.2 through §312.8, and §312.10. EPC has consistently maintained a high standard of compliance for member companies, and although the changes to existing guidelines are minimal, the attached Exhibit III is proof that EPC will continue to meet and exceed the requirements of the revised COPPR. Furthermore, to ensure greater transparency to this process, EPC submits this document without marking it as a "confidential."

(3) In addition to the documents submitted hereunder, member companies agree to cooperate with all of EPC's reviews and inquiries. Through its Consumer Online Hotline, EPC works closely with members and consumers to resolve any and all privacy-related disputes in a fair and expeditious manner. Upon joining EPC, member companies are required to nominate a "user grievance coordinator", who shall be responsible for the initial fielding of all consumer privacy complaints. In addition, member companies are required to provide consumers with a simple and effective way to submit their privacy concerns directly to the member company (e.g., via email or an online form.) To further ensure consumers questions or concerns are satisfactorily addressed, member companies are required to include EPC contact information in their privacy policies.
EPC does maintain the right, as provided for under §312.11(3), to take disciplinary action against member companies for non-compliance with EPC's self-regulatory program requirements. If EPC determines, in good faith and in its sole discretion, that a member company has failed within a reasonable period to cure any material noncompliance with any program requirements, EPC reserves the right to immediately terminate their membership in the program.

Where there has been a continued demonstration of noncompliance (willful or otherwise), EPC reserves the right to investigate and issue a fine which would result in a "voluntary payment" under §312.11(b)(3)(iii).
However, it should be noted, for the record, that EPC is fully aware that each and every member company has voluntarily joined and maintained membership in the COPPA Safe Harbor program without incident. EPC is dedicated to continuing its closely working relationship with each and every member company to ensure the high standard of compliance.

(D) – Explanation of ESRB Privacy Certified Annual Reporting process (pursuant to 312.11(d))

As indicated in the attached Participation Agreement (Exhibit II), member companies receive bi-annual compliance reports (i.e., assessments), a sample of which has also been attached hereto for reference (Exhibit IV – marked "CONFIDENTIAL"). To fulfill its obligation under §312.11(d), EPC will provide the Commission with a similar report, i.e. a compilation of all required and recommended issues cited throughout the year along with the number of times each issue was cited. At no time will EPC's annual reporting disclose specific information about any member company, including but not limited to company name, URL, or title of app.
To the extent that any consumer complaints or concerns are reported, whether through EPC's Consumer Online Hotline or any other means, such information will be included in an accompanying Consumer Complaint summary. Again, EPC will not disclose specific information about any member company as it may relate to any complaint.

(E) – Additional Supporting Documentation

To provide the Commission with further insight about EPC's program, the following documents are attached for review and reference, however all marked CONFIDENTIAL:

- *Self-Assessment Questionnaire (Exhibit V):* as mentioned earlier, this document is used to assist EPC in its initial upfront and detailed assessment of a company's websites, mobile apps, etc. The specific content of this questionnaire is reviewed and updated on a regular basis to ensure it incorporates any new laws and/or best practices that may directly affect how companies collect, share and use personal information
- *Amended COPPA Rule Self-Assessment Questionnaire (Exhibit VI)*: soon after the Commission released the final COPPA Rule in December, this document was distributed to member companies in order to assist EPC in providing each member company with a customized report detailing any material changes they would be required to make in order to be compliant with amended Rule.
- *Amended COPPA Rule Checklist (Exhibit VII)*: this document is provided to each member company to assist with ongoing compliance, whether at the initial development of new websites or apps, or to understand how existing websites or apps need to change in order to maintain compliance with the amended Rule.

EXHIBIT II

ESRB Privacy Certified Kids Seal Requirements

(highlighted text indicate material changes to existing Program Requirements)

The following outlines the ESRB Privacy Certified Kids Seal Requirements ("Program Requirements") as referenced in the ESRB Privacy Certified Participation Agreement ("Agreement"). Any defined terms used in the Agreement shall have the same meaning when utilized here. If any of Participant's Monitored Web Sites or Mobile Apps are directed at and/or collect Personally Identifiable Information from children under the age of thirteen (13), or if any section of Participant's Monitored Web Sites or Mobile Apps are directed at, targeted at, and/or collects Personally Identifiable Information from children under the age of thirteen (13), or if Participant has actual knowledge that it is collecting or maintaining Personally Identifiable Information from children under the age of thirteen (13) through its Monitored Web Sites or Mobile Apps, Participant must comply with the following ESRB Privacy Certified Kids Seal Requirements. If any of Participant's Monitored Web Sites or Mobile Apps are collecting information from citizens of the EU and Participant has enrolled in the EU Privacy Seal Program, Participant must also comply with the ESRB Privacy Certified EU Seal Requirements, which shall, by reference, incorporate any and all applicable rules and definitions as outlined under the Children's Online Privacy Protection Act (as amended on December 19, 2012.)

I. DEFINITIONS

Child/Children means users resident in the United States, Canada or anywhere else in the world, who are under thirteen (13) years of age.

Online Information Practices encompass, but are not limited to: (i) Participant's practices regarding consumer notification and consumer access to their personal information; (ii) Participant's practices with respect to the collection, use or disclosure of personal information; (iii) Participant's practices regarding user choice and consent to how personal information is used or shared; and (iv) security measures taken to protect information provided by users.

Parent shall include legal guardian.

Personally Identifiable Information means any information that can be used to identify an individual or which enables direct contact with an individual. This would include an individual's name, online contact information (i.e. email addresses or other identifier that permits direct online contact with a person via instant messaging, video, voice over internet protocol or any other means not specifically defined herein), phone number, fax number, home address, social security number, driver's license number, credit card number, photos, videos, or audio containing the image or voice of a child, persistent identifiers (such as a customer number held in a cookie or a processor serial number, a unique device identifier, or IP address), or geolocation information sufficient to identify a street name and name of town. Demographic information that is combined with personal information (including, but not limited to, gender, educational background, or political affiliation) also becomes Personally Identifiable Information. Personally Identifiable Information does not include information that is encoded or rendered anonymous, or publicly available information that has not been combined with non-public

Personally Identifiable Information (and has not been previously defined as Personally Identifiable Information.)

Privacy Risk Assessment means the initial, pre-certification report provided by ESRB to a company before it becomes a Participant in the Program. This report reflects ESRB's assessment of the legal and business risks posed by the company's then-current Privacy Statement, data gathering practices and online privacy disclosures.

Privacy Statement means the statement, posted on the Monitored Web Sites or Mobile Apps, which discloses Participant's policies regarding user privacy and Participant's practices with respect to the collection, use and disclosure of Personally Identifiable Information, as such practices may be updated from time to time.

II. PROGRAM DOCUMENTS AND PROCEDURES

A. Initial SAQ/Certification Report

If it has not already done so during the pre-certification phase in anticipation of receipt of ESRB's Privacy Risk Assessment, Participant shall fully complete a Self Assessment Questionnaire ("SAQ") and return it to ESRB. In providing the completed SAQ, Participant understands that ESRB may rely on the statements contained therein for the purpose of determining Participant's information collection practices as well as Participant's overall qualification for the ESRB Privacy Online Program. An authorized representative of Participant shall sign and attest that the information provided in the SAQ is true and accurate as of the date submitted.

ESRB shall review the completed SAQ, along with Participant's Privacy Statement and related information collection practices, and assess the state of Participant's overall compliance with the Program Requirements. Upon completing this review, ESRB will provide Participant with a comprehensive report detailing any and all required changes to Participant's Privacy Statement and/or Monitored Web Sites or Mobile Apps ("Certification Report"). Participant must implement all changes required by the Certification Report and attest to ESRB that it has done so by returning a signed copy of the Certification Report. ESRB will then complete a final review of the Monitored Web Sites or Mobile Apps and, if all the required changes have been implemented, provide Participant with access to the Marks.

B. Onsite Compliance Reviews

1. At the time Participant is certified to enter the Program, Participant shall be subject to an onsite compliance review by ESRB. The onsite review shall be scheduled in advance for a mutually-convenient time and shall be conducted during Participant's normal business hours.

2. Should Participant's compliance record or ongoing concerns with respect to the Monitored Web Sites or Mobile Apps so warrant, ESRB may conduct additional onsite reviews, the necessity of which shall be determined by ESRB in its sole discretion.

Participant shall reimburse ESRB for the reasonable costs associated with any such onsite review.

3. Participant may also request additional onsite visits by ESRB (e.g., for staff training or educational purposes).

C. Biannual Monitoring and Compliance Reports

Twice a year ("Reporting Periods") during the Term of the Agreement, ESRB shall provide Participant with a report ("Compliance Report") that will: (i) list all of the Monitored Web Sites or Mobile Apps as well as any new sites or mobile apps that have come to ESRB's attention during that Reporting Period; (ii) describe changes to Participant's Privacy Statement and/or Monitored Web Sites or Mobile Apps which are necessary for Participant to remain compliant with the Program Requirements; and (iii) propose changes which, although not required under the Program Requirements, reflect "best practices" which are highly recommended by ESRB. Within three (3) weeks of Participant's receipt of a Compliance Report, Participant must notify ESRB, through ESRB's SharePoint system (or through whatever other means may be specified by ESRB pursuant to its then-current policy), that Participant has implemented all changes required by the Compliance Report. If Participant needs more than three weeks to implement the required changes, Participant shall notify ESRB immediately and provide a time frame within which it commits to complete all changes.

In order for ESRB to provide thorough and accurate Compliance Reports, Participant must provide ESRB full access to the Monitored Web Sites or Mobile Apps, including access to "members only" or password-protected areas of the Monitored Web Sites or Mobile Apps.

III. CONTINUING OBLIGATIONS OF PARTICIPANT

A. Designation of Site Coordinator

At the time the Agreement is executed, Participant shall name a coordinator for the Monitored Web Sites or Mobile Apps ("Site Coordinator") who shall be ESRB's contact, and Participant shall keep ESRB apprised should it designate a different individual to act as Site Coordinator. The Site Coordinator shall be the employee responsible for the effectuation and implementation of the Privacy Statement and compliance with these Program Requirements. All notices from ESRB shall be directed to the Site Coordinator.

B. Notifying ESRB of Material Changes

1. Participant is required to notify ESRB in advance of any material change(s) to its Online Information Practices, including, by way of example, changes to Participant's Terms of Use or End User License Agreement; changes to its data security infrastructure; or the roll-out of any new sweepstakes, contest or similar promotion on a Monitored Web Site or Mobile App.

2. Participant must obtain prior approval from ESRB for any substantive modification to its Privacy Statement, whether such modification results from a material change in Participant's Online Information Practices, the revamping of a Monitored Web Site or Mobile App, or otherwise.

3. Where changes to Participant's Monitored Web Sites or Mobile Apps, Privacy Statement or Online Privacy Practices have been implemented, Participant may be required to submit an updated SAQ or provide updated information in a form determined by ESRB. Participant may also be required to submit a new SAQ if Participant has undergone a "change in control," as defined in Section 2.5 of the Agreement, or if there has been an investigation of Participant's practices by a federal or state authority, agency or regulatory body or any unit of federal or state government.

C. Notifying Users of Material Changes

Participant is required to notify users of any material change(s) in its Online Information Practices or Privacy Statement. Notice should be provided to users prior to the change taking effect. Participant shall give ESRB advance notice of any material change so that ESRB may ensure that users are properly notified. Different types of material changes may require different forms of notice to users. If, while reviewing Participant's Monitored Web Sites in the normal course, ESRB discovers a material change of which it was not previously notified, ESRB will advise Participant in the next scheduled Compliance Report of the type of notice Participant must provide to users of the Monitored Web Sites or Mobile Apps.

D. Resolution of Consumer Complaints

1. Participant must implement procedures to receive, investigate and resolve privacy inquiries and complaints from users. Where Participant's internal mechanisms are unable to address a user grievance effectively, Participant shall refer the user to ESRB and advise the user of ESRB's Dispute Resolution process.

2. ESRB shall maintain a consumer online hotline which visitors to Participant's Monitored Web Sites or Mobile Apps may contact with inquiries or complaints regarding these sites. After determining the nature of the complaint, ESRB shall respond in one of the following ways. If the question, concern or complaint is not privacy-related, ESRB shall forward the email to the individual at Participant's company designated for such purpose. If the consumer's email is privacy-related and presents a question or an issue ESRB can independently address, ESRB shall respond directly to the consumer. If analysis and/or resolution of the consumer's complaint requires input from Participant, ESRB shall contact Participant to obtain the necessary information. Participant shall cooperate with ESRB in resolving consumer complaints.

3. If neither Participant nor ESRB succeeds in independently resolving a consumer grievance, and the consumer wishes to pursue the matter further, Participant agrees to fully participate, along with the consumer, in ESRB's Dispute Resolution process and agrees to accept ESRB's judgment as final.

E. Required Notice to ESRB

Participant shall notify ESRB in writing within thirty (30) days if Participant: (i) changes its name; (ii) undergoes a "change in control," as defined in Section 2.5 of the Agreement; or (iii) changes the domain name of any Monitored Web Site or Mobile App.

IV. PRIVACY STATEMENT

A. Content of General Privacy Statement

Participant shall maintain and abide by a Privacy Statement that is either written by Participant and approved by ESRB, in its sole discretion, or written by ESRB. The Privacy Statement shall clearly set forth Participant's Online Information Practices. The Privacy Statement must link only to and from web pages that are in the English language. At a minimum, Participant's posted Privacy Statement shall provide disclosure to users with respect to each of the following elements:

1. notice that the site is a participant in the ESRB Privacy Online Program;
2. a full description of how users of the site can contact Participant;
3. a full description of how users of the site can contact ESRB with questions or concerns about Participant's Privacy Statement or privacy practices;
4. a description of the Personally Identifiable Information that is collected through the site;
5. the identity (including name, address and e-mail address) of all of the organizations (i.e. third parties) that are collecting Personally Identifiable Information through the site;
6. the manner in which Personally Identifiable Information collected through the site will be used;
7. the entities (if any) with whom Personally Identifiable Information collected through the site is shared, and the entities that collect or maintain information on behalf of the site or app;
8. notice of whether Participant supplements Personally Identifiable Information collected on the site with information from other sources;
9. disclosure of the tracking technologies, if any, used on the site either by Participant or by an authorized third party;
10. an explanation of when and how users may exercise opt-in and/or opt-out options;
11. the nature of the security measures in place on the site;
12. notice that Personally Identifiable Information provided to Participant may be subject to disclosure in response to judicial or other government subpoenas, warrants, or orders;
13. notice that information posted by users in online bulletin boards, chat rooms, news groups or other public forums may be displayed publicly;
14. the notification procedures to be utilized by Participant in the event of a material change in its Online Information Practices and/or Privacy Statement; and

15. disclosure of the last date on which the Privacy Statement was updated (i.e., "updated as of").

B. Content of Kids Privacy Statement

If Participant is collecting Personally Identifiable Information from Children, or if any portion of Participant's Monitored Web Sites or Mobile Apps are directed to or target Children, then Participant either must implement a separate Kids Privacy Statement, or incorporate into its General Privacy Statement a section specifically devoted to Participant's Online Information Practices with respect to Children. In addition to the elements set forth in Section IV.A. above, Participant's Kids Privacy Statement, or, if there is no separate Kids Statement, that portion of Participant's General Privacy Statement reflecting its Online Information Practices with respect to Children, must contain the following elements:

1. Disclosure of the manner in which Children's Personally Identifiable Information is collected through the site or app and how it will be used, whether with Participant or third party acting on behalf of Participant, including but not limited to use for purposes of fulfilling a requested transaction, for record keeping purposes, or for the purpose of marketing products or services to the Child;

2. Notice that a Child's participation in a chat room, bulletin board, or other online forum provided by Participant may result in such Child's public disclosure of Personally Identifiable Information, and notice of Participant's policy to remove any such Personally Identifiable Information if and when discovered, including but not limited to any information that may have been shared with a third party;

3. Notice that a parent has the option to consent to Participant's collection and use of their Child's Personally Identifiable Information without consenting to Participant's disclosure of that information to third parties;

4. A description of the procedures pursuant to which parents can prevent Participant's disclosure of their Child's Personally Identifiable Information to third parties;

5. Disclosure that Participant may not condition a Child's participation in an activity on such Child disclosing more Personally Identifiable Information than is reasonably necessary to participate in such activity;

6. Notice that parents may view and elect to remove their Child's Personally Identifiable Information and may also refuse to allow Participant to further collect or use their Child's Personally Identifiable Information; and

7. A description of the process by which a parent can, for any purpose, access and view their Child's Personally Identifiable Information, including for the purpose of preventing disclosure to third parties of their Child's Personally Identifiable Information.

C. Placement of Kids Privacy Statement and ESRB Marks

Participant must provide, on its home page and on any pages where Personally Identifiable Information is collected from Children, a link to its Kids Privacy Statement or to that portion of its General Privacy Statement that reflects Participant's Online Information Practices with respect to Children. Participant should label this link with the "Kids Privacy Seal" Mark identified on Schedule D. If it is not possible to use this Mark in a given location, ESRB may, in the exercise of its discretion, permit use of hyperlink text with the phrase "Kids Privacy Policy" or its approved equivalent. The Kids Seal must link directly to Participant's Kids Privacy Statement or the portion of Participant's Privacy Statement describing Participant's Online Information Practices with respect to Children. Participant must provide, at the top and/or bottom of Participant's Kids Privacy Statement, a clearly labeled link to Participant's General Privacy Statement.

V. DIRECT NOTICE AND PARENTAL CONSENT REQUIREMENTS

A. Direct Notice to Parents to Obtain Prior Verifiable Parental Consent

1. Participant must make reasonable efforts, taking into account available technology, to ensure that a parent receives notice of Participant's Online Information Practices with respect to Children, including notice of any material change in the Online Information Practices of Participant to which the parent has previously consented. With limited exceptions, Participant must provide notice to parents and obtain verifiable parental consent *before* collecting any Personally Identifiable Information from a Child or materially changing its use of previously collected data or new data collection practices. For exceptions to this requirement, see Section V.D. below.

2. Direct notice to Parents sent to obtain prior verifiable parental consent must contain: (i) a hyperlink to Participant's Kids Privacy Statement (or that portion of Participant's General Privacy Statement that reflects its Online Information Practices with respect to Children) and notice that Participant has collected the parent's online contact information from the child, and, if such is the case, the name of the parent or child, in order to obtain parental consent; (ii) disclosure of the additional items of Personally Identifiable Information that the Participant intends to collect; (iii) disclosure that Participant must obtain the parent's permission to collect and use the Personally Identifiable Information from the Child; (iv) a description of the procedures by which a parent may give Participant such permission; and (v) notice that if the parent does not provide consent within a reasonable time, Participant will delete the parent's online contact information from its records.

B. Mechanisms for Obtaining Verifiable Parental Consent

Participant must take reasonable measures, in light of available technology, to ensure that the person providing consent is the Child's Parent. Acceptable mechanisms for

obtaining verifiable parental consent include: (i) providing a consent form to be signed by the Parent and returned to Participant by mail, scan, or fax; (ii) requiring a Parent to use a credit card in connection with a transaction on Participant's site; (iii) having a Parent call a toll-free telephone number staffed by trained personnel; (iv) having a Parent connect to trained personnel via video-conference; (v) verifying the Parent's identity by checking a form of government-issued identification against databases of such information, provided that the identification information is deleted immediately after verification; or (vi) using e-mail accompanied by a PIN or password obtained by the parent through one of the verification methods described above. For purposes of clarification, except for option (ii) above, the Parent shall be provided just-in-time notification that any information collected for the purpose of parental consent shall be collected solely for the purpose of obtaining parental consent, and that this collection may involve the use of a third party; however, this third party shall only share this data with Participant and shall not share, sell, or use, in any other manner, the information collected for the purposes indicated in this paragraph. Participant must provide Parent the option to consent to the collection and use of the child's Personally Identifiable Information without consenting to disclosure of his or her personal information to third parties.

C. Information Collected for Participant's Internal Use Only

Where Participant's use of Personally Identifiable Information is for internal purposes only (i.e. "voluntary"), and there is no disclosure to third parties or the public, methods to obtain prior verifiable parental consent may also include use of email, coupled with additional steps to provide assurances that the person providing the consent is the Parent. Such additional steps include: sending a delayed confirmatory email to the Parent after receiving consent or obtaining a postal address or telephone number from the Parent and confirming the parent's consent by letter or telephone call. If Participant implements such methods, Participant must provide notice in the confirmation communication that the Parent can revoke any consent given in response to the earlier email, coupled with instructions on how to revoke such consent.

D. Exceptions to Obtaining Prior Verifiable Parental Consent

Participant may collect a Child's name or email address prior to obtaining parental consent under the following exceptions:

1. **Obtaining Consent:** Participant may collect the name or online contact information of a Parent or child for the sole purpose of obtaining parental consent; provided, however, that if Participant does not obtain parental consent after a reasonable time from the initial date of collection, Participant shall permanently delete collected information from Participant's records. Participant must not use the collected name or email address to re-contact the Parent or Child.

2. **Internal Uses (Voluntary collection):** Participant may collect the name or online contact information of the Parent solely to update the Parent about the Child's participation in a website or online service that does not otherwise collect, use, or share the Child's Personally Identifiable Information. Participant must ensure that the Parent receives notice as described herein under section V(C).

3. **One-Time Response:** Participant may collect the online contact information from a child for the sole purpose of responding directly, on a one-time basis, to a specific request from the child -- so long as such information is not used to re-contact the child or for any other purpose and is subsequently deleted from Participant's records. Under this exception, Participant is not required to provide direct notice to a Parent or to obtain verifiable parental consent.

4. **Multiple Responses:** Participant may collect the online contact information of a Child and Parent in order to respond directly, on more than one occasion, to a specific request from the Child, so long as such information is not used for any other purpose. In such instances, Participant must make reasonable efforts, taking into consideration available technology, to give direct notice to Parents, which must: (i) include Participant's Kids Privacy Statement or that portion of Participant's General Privacy Statement that reflects its Online Information Practices with respect to Children; (ii) explain to the Parent that Participant has collected the Child's email address to respond to the Child's request; (iii) explain that the Child's request will require more than one contact with the Child; (iv) explain that the Parent may refuse to permit further contact with the Child and may require Participant to delete the Child's information; (v) explain how a Parent can refuse to permit further contact and information collection from the Child; and (vi) explain that if the Parent does not respond, Participant may not use the collected information for the purposes stated in the direct notice. This direct notice to Parents must be sent immediately after Participant's initial response to the Child and before sending any additional responses.

5. **Protecting Child Safety:** Where Participant has used reasonable efforts to provide notice to the Parent, Participant may collect a Child's or Parent's name and online contact information to the extent reasonably necessary to protect the safety of the Child on a Monitored Web Site or Mobile App, provided such information is used for the sole purpose of protecting the Child's safety and not used to re-contact the Child or for any other purpose. In such cases, Participant must make reasonable efforts, taking into consideration available technology, to give direct notice to Parents, which must: (i) include Participant's Kids Privacy Statement or that portion of Participant's General Privacy Statement that reflects its Online Information Practices with respect to Children; (ii) explain that Participant has collected the Child's name and online contact information to protect the Child's safety; (iii) explain that the Parent may refuse to permit further contact with the Child and may require Participant to delete the Child's information; (iv) explain how the Parent can refuse to permit further contact and information collection from the Child; and (v) explain that if the Parent does not respond, Participant may use the information for the purposes stated in the direct notice.

6. **Protecting Others:** Participant may collect a Child's online contact information to protect the integrity or security of Participant's Monitored Web Sites or Mobile Apps, to take precautions against liability, to respond to judicial process, or to provide information to law enforcement agencies or pursuant to authorized investigations on matters related to public safety, provided such information is not used for any other purpose. Under this exception, Participant is not required to provide direct notice to Parents.

VI. PROVIDING PARENTS ACCESS TO AND CONTROL OVER CHILDREN'S PERSONALLY IDENTIFIABLE INFORMATION

Participant must provide Parents with the opportunity to control the use of their Child's Personally Identifiable Information as well as access to the following information:

- the specific information Participant and/or any third parties, has collected from the Child, including his/her name, address, telephone number, hobbies, etc;
- an opportunity for the Parent to prevent Participant and/ or any third party, from collecting or using Personally Identifiable Information about their child in the future; and
- an opportunity for the Parent to direct Participant to delete their Child's Personally Identifiable Information from Participant's and/or any third party's records.

Participant must take reasonable measures, in light of available technology, to ensure that the person requesting access to or providing instructions about the Child's Personally Identifiable Information is the Child's parent. For acceptable verification mechanisms, refer to Section V.B. above.

Neither Participant nor any third party shall be held liable for any disclosure made in good faith and following the procedures set forth herein in responding to a request for disclosure of any Personally Identifiable Information under this paragraph.

VII. DATA COLLECTION AND SECURITY

A. Participant shall, upon ESRB's reasonable request, provide details regarding how Personally Identifiable Information is gathered from and/or tracked through Participant's Monitored Web Sites or Mobile Apps, as well as disclosure regarding how such Personally Identifiable Information is utilized.

B. Participant must establish, implement and maintain reasonable procedures to protect the confidentiality, security and integrity of Personally Identifiable Information within its control, whether collected from adults or children, from unauthorized access, use, alteration, distribution or disclosure. Participant shall utilize appropriate, commercially reasonable methods (e.g., encryption) to protect any sensitive information it collects, such as social security numbers or transactional information, including but not limited to financial information. Participant must also take reasonable steps to release Children's Personally Identifiable Information only to service providers and third parties that are capable of maintaining the confidentiality, security, and integrity of such information, and who provide written assurances that they will maintain the Children's Personally Identifiable Information in such a manner.

C. Participant shall take reasonable steps when collecting, creating, maintaining, using, distributing or disclosing Personally Identifiable Information to assure that the data created, utilized and/or shared is up-to-date, complete and accurate.

D. Participant must implement reasonable and effective processes and/or mechanisms which allow users to correct material inaccuracies in Personally Identifiable Information, such as account or contact information. These processes and/or mechanisms must

be easily comprehended and "user-friendly" and, once utilized, must confirm to users that the cited inaccuracies have been corrected.

E. If Participant's Monitored Web Sites or Mobile Apps provide links to third-party web sites, Participant must implement "exit messages" or "bumper pages" wherever users travel via such links to a third-party site to inform a user that: (i) he/she is leaving Participant's web site; and (ii) Participant's Terms of Use and Privacy Statement will no longer be applicable upon user's departure from Participant's web site. Prior to implementation, Participant must submit the specific language it intends to utilize for this purpose to ESRB for approval.

EXHIBIT III

ESRB Privacy Certified Program
Participation Agreement

EXHIBIT IV – SAMPLE COMPLIANCE REPORT

EXHIBIT V – SELF ASSESSMENT QUESTIONNAIRE

*** CONFIDENTIAL ***

EXHIBIT VI

AMENDED COPPA RULE SELF-ASSESSMENT QUESTIONNAIRE

EXHIBIT VII – AMENDED COPPA RULE CHECKLIST