OFFICE OF THE
CHAIRWOMAN

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

August 16, 2013

The Honorable Mary L. Landrieu
Chairwoman
Committee on Small Business & Entrepreneurship
United States Senate
428A Russell Senate Office Building

Dear Chairwoman Landrieu:

We submit this sixth annual report in accordance with Section 212(a)(6) of the amended Small Business Regulatory Enforcement Fairness Act ("SBREFA"). SBREFA requires agencies to publish guides to assist small entities in complying with rules that significantly affect them. The Federal Trade Commission ("Commission" or "FTC") has a longstanding and effective business education program[1] and only a small fraction of our business compliance library is discussed in this report.

Since we submitted our fifth annual SBREFA report (which covered the time period from July 1, 2011, to July 1, 2012), the FTC has issued one final rule that is subject to Section 212 of SBREFA[2]:

- **Children's Online Privacy Protection Rule ("COPPA Rule"), 16 C.F.R. Part 313**: On December 19, 2012, the Commission issued the final amended COPPA Rule, modifying the definitions of operator, personal information, and Web site or online service directed to children. 78 Fed. Reg. 3,972 (Jan. 17, 2013). The amendment also updates the requirements set forth in the notice, parental consent, confidentiality and security, and safe harbor provisions, and adds a new provision addressing data retention

[1] From FY2002 - FY2011, the FTC's "Compliance Assistance" under SBREFA was rated an "A" by the Small Business Administration's National Ombudsman. We anticipate the same grade when the National Ombudsman submits its FY2012 SBREFA Report for all agencies.

[2] Section 212 requires agencies to publish a "small entity compliance guide" for any new rule for which an agency is required to prepare a final regulatory flexibility analysis under section 3(a) of the Regulatory Flexibility Act, which is codified at 5 U.S.C. § 604.

and deletion. The amendments became effective on July 1, 2013. In April 2013, the Commission staff made available updated COPPA guidance. The document, titled

"Complying With COPPA: Frequently Asked Questions,"[3] contains information directed to Web sites and online services whose work online may involve the collection of personal information from children under the age of thirteen. The Commission also made available "The Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business" (July 2013).[4] These materials supplement the Rule and other COPPA-related material previously published by the FTC.

Over the past year, the Commission also certified to the Small Business Administration that certain other final regulations issued would not have a significant economic impact on a substantial number of small business entities. Nonetheless, the Commission published a Final Regulatory Flexibility Act Analysis ("FRFA") along with these final regulations. We have either made available or are preparing updated compliance materials for each of these rulemakings, although not required to do so by SBREFA. One example is below:

- **Energy and Water Use Labeling For Consumer Products Under the Energy Policy and Conservation Act ("Energy Labeling Rule"), 16 C.F.R. 305**: The Energy Labeling Rule requires manufacturers of certain appliances to disclose a product's annual energy cost or efficiency information — which are based on Department of Energy ("DOE") test procedures — on EnergyGuide labels, and to report these findings to the FTC. In January 2013, the Commission amended the Rule by streamlining data reporting requirements for manufacturers, clarifying testing requirements and enforcement provisions, improving online energy label disclosures, and making several minor technical changes and corrections.[5] 78 Fed. Reg. 2,200. Later, in February 2013, the Commission added disclosure requirements to the Rule to help consumers, distributors, contractors, and installers easily determine whether a specific furnace or central air conditioner meets applicable DOE regional efficiency standards. 78 Fed. Reg. 8,362.

---

[3] The document is enclosed and is found at http://business.ftc.gov/documents/Complying-with-COPPA-Frequently-Asked-Questions. FTC staff further updated and expanded the guidance in June and July 2013 and will continue to add to the document as appropriate.

[4] The document is enclosed and is found at http://business.ftc.gov/documents/bus84-childrens-online-privacy-protection-rule-six-step-compliance-plan-your-business.

[5] The Rule's title was also changed from "Part 305—Rule Concerning Disclosures Regarding Energy Consumption and Water Use of Certain Home Appliances and Other Products Required Under the Energy Policy And Conservation Act ('Appliance Labeling Rule')" to "Part 305—Energy And Water Use Labeling For Consumer Products Under The Energy Policy and Conservation Act ('Energy Labeling Rule')."

To reflect these rule changes, the FTC revised our publications, "EnergyGuide Labeling: FAQs for Appliance Manufacturers,"[6] in May 2013, and "EnergyGuide Labels: Templates for Manufacturers" in July 2013.[7]

Finally, the Commission updated business compliance materials for Final Rule actions even where an FRFA was not prepared. Examples include the following:

- **Used Motor Vehicle Trade Regulation Rule ("Used Car Rule"), 16 C.F.R. Part 455**: The FTC's Used Car Rule requires dealers to post a Buyers Guide in every used car they offer for sale. The Used Car Rule also requires dealers to use Spanish-language versions of the Buyers Guide and to make related contract disclosures in Spanish when they conduct sales in Spanish. The Commission issued a Final Rule that made minor corrections to the Spanish translation of the Buyers Guide. The revised Spanish-language versions took effect in February 2013, but dealers were allowed to use up any remaining supplies of the current Buyers Guide. The revised Spanish translations are enclosed and can be found on the FTC's website at business.ftc.gov.[8] "Fillable" versions of the Buyers Guide in English and Spanish are now available.

- **Red Flags Rule, 16 C.F.R. 681**: The Commission and banking agencies promulgated the Red Flags Rule in 2007. The Red Flag Program Clarification Act of 2010, Pub. L. No. 111-319, narrowed the definition of "creditors" covered by the Rule. The Commission published an Interim Final Rule to implement this legislation in December 2012. 77 Fed. Reg. 72,712. The amendment provided that a creditor is covered only if, in the ordinary course of business, it regularly obtains or uses consumer reports in connection with a credit transaction; furnishes information to consumer reporting agencies in connection with a credit transaction; or advances funds to or on behalf of a person, in certain cases. The comment period closed in February 2013, and the Interim Final Rule became final at that time. The Commission published "Fighting Identity Theft with the Red Flags Rule: A How-To Guide for Business,"[9] which has tips for organizations under the FTC's jurisdiction to determine whether they need to design an identity theft prevention program.

---

[6] The document is enclosed and is found at: http://business.ftc.gov/documents/bus-82-energyguide-labels-faqs.

[7] This can be found at http://business.ftc.gov/documents/energyguide-labels-template.

[8] Please see http://business.ftc.gov/documents/gu%C3%ADa-del-comprador-version-para-llenar and http://business.ftc.gov/documents/gu%C3%ADa-del-comprador-con-notas-sobre-el-formato.

[9] The document is enclosed and is found at: http://www.business.ftc.gov/documents/bus23-fighting-identity-theft-red-flags-rule-how-guide-business.

For many years, the FTC has had a highly effective program of providing compliance assistance to small businesses.[10] We plan to continue to refine and improve these efforts. If you have any questions, please contact Christian S. White, the Deputy General Counsel for Legal Counsel and Small Business Coordinator at the Commission, at (202) 326-2476.

Sincerely,

/signed/
Edith Ramirez
Chairwoman

Enclosures

cc: The Honorable Sam Graves
Chairman
Committee on Small Business
U.S. House of Representatives
2361 Rayburn House Office Building
Washington, D.C. 20515

[10] The Commission also considers the specific and unique circumstances of a case when enforcinge business obligations. Section 223 of SBREFA (1996) requires that agencies establish policies to reduce or waive penalties for small entities in appropriate circumstances. In 1997, the Commission issued a small business leniency policy statement that describes factors that may result in reduction or waiver of penalties. *See* 62 Fed. Reg. 16,809 (Apr. 8, 1997) (issuing policy); 62 Fed. Reg. 46,363 (Sept. 2, 1997) (responding to comment received). As such cases arise, the Commission considers these leniency factors whenever a civil penalty may be assessed against a small business.

In addition, and beyond SBREFA requirements, the Commission established corporate leniency policies for violations of the Textile and Wool Rules, 67 Fed. Reg. 71,566 (Dec. 2, 2002), the Funeral Rule (through the Funeral Rule Offender Program), and the Franchise Rule (through the Franchise Rule Alternative Law Enforcement Program) that have helped in fostering a more cooperative, less threatening regulatory environment for small entities. These policies have helped increase overall compliance with the rules while minimizing the burden on business of correcting certain minor or inadvertent errors that are not likely to injure consumers.

OFFICE OF THE
CHAIRWOMAN

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

August 15, 2013

The Honorable Sam Graves
Chairman
Committee on Small Business
U.S. House of Representatives
2361 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Graves:

We submit this sixth annual report in accordance with Section 212(a)(6) of the amended Small Business Regulatory Enforcement Fairness Act ("SBREFA"). SBREFA requires agencies to publish guides to assist small entities in complying with rules that significantly affect them. The Federal Trade Commission ("Commission" or "FTC") has a longstanding and effective business education program[1] and only a small fraction of our business compliance library is discussed in this report.

Since we submitted our fifth annual SBREFA report (which covered the time period from July 1, 2011, to July 1, 2012), the FTC has issued one final rule that is subject to Section 212 of SBREFA[2]:

- **Children's Online Privacy Protection Rule ("COPPA Rule"), 16 C.F.R. Part 313**: On December 19, 2012, the Commission issued the final amended COPPA Rule, modifying the definitions of operator, personal information, and Web site or online service directed to children. 78 Fed. Reg. 3,972 (Jan. 17, 2013). The amendment also updates the requirements set forth in the notice, parental consent, confidentiality and security, and safe harbor provisions, and adds a new provision addressing data retention and deletion. The amendments became effective on July 1, 2013. In April 2013, the Commission staff made available updated COPPA guidance. The document, titled "Complying With COPPA: Frequently Asked Questions,"[3] contains information directed

[1] From FY2002 - FY2011, the FTC's "Compliance Assistance" under SBREFA was rated an "A" by the Small Business Administration's National Ombudsman. We anticipate the same grade when the National Ombudsman submits its FY2012 SBREFA Report for all agencies.

[2] Section 212 requires agencies to publish a "small entity compliance guide" for any new rule for which an agency is required to prepare a final regulatory flexibility analysis under section 3(a) of the Regulatory Flexibility Act, which is codified at 5 U.S.C. § 604.

[3] The document is enclosed and is found at http://business.ftc.gov/documents/Complying-with-COPPA-Frequently-Asked-Questions. FTC staff further updated and expanded the guidance in June and July 2013 and will continue to add to the document as appropriate.

to Web sites and online services whose work online may involve the collection of personal information from children under the age of thirteen. The Commission also made available "The Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business" (July 2013).[4] These materials supplement the Rule and other COPPA-related material previously published by the FTC.

Over the past year, the Commission also certified to the Small Business Administration that certain other final regulations issued would not have a significant economic impact on a substantial number of small business entities. Nonetheless, the Commission published a Final Regulatory Flexibility Act Analysis ("FRFA") along with these final regulations. We have either made available or are preparing updated compliance materials for each of these rulemakings, although not required to do so by SBREFA. One example is below:

- **Energy and Water Use Labeling For Consumer Products Under the Energy Policy and Conservation Act ("Energy Labeling Rule"), 16 C.F.R. 305**: The Energy Labeling Rule requires manufacturers of certain appliances to disclose a product's annual energy cost or efficiency information — which are based on Department of Energy ("DOE") test procedures — on EnergyGuide labels, and to report these findings to the FTC. In January 2013, the Commission amended the Rule by streamlining data reporting requirements for manufacturers, clarifying testing requirements and enforcement provisions, improving online energy label disclosures, and making several minor technical changes and corrections.[5] 78 Fed. Reg. 2,200. Later, in February 2013, the Commission added disclosure requirements to the Rule to help consumers, distributors, contractors, and installers easily determine whether a specific furnace or central air conditioner meets applicable DOE regional efficiency standards. 78 Fed. Reg. 8,362. To reflect these rule changes, the FTC revised our publications, "EnergyGuide Labeling: FAQs for Appliance Manufacturers,"[6] in May 2013, and "EnergyGuide Labels: Templates for Manufacturers" in July 2013.[7]

Finally, the Commission updated business compliance materials for Final Rule actions even where an FRFA was not prepared. Examples include the following:

---

[4] The document is enclosed and is found at http://business.ftc.gov/documents/bus84-childrens-online-privacy-protection-rule-six-step-compliance-plan-your-business.

[5] The Rule's title was also changed from "Part 305—Rule Concerning Disclosures Regarding Energy Consumption and Water Use of Certain Home Appliances and Other Products Required Under the Energy Policy And Conservation Act ('Appliance Labeling Rule')" to "Part 305—Energy And Water Use Labeling For Consumer Products Under The Energy Policy and Conservation Act ('Energy Labeling Rule')."

[6] The document is enclosed and is found at: http://business.ftc.gov/documents/bus-82-energyguide-labels-faqs.

[7] This can be found at http://business.ftc.gov/documents/energyguide-labels-template.

- **Used Motor Vehicle Trade Regulation Rule ("Used Car Rule"), 16 C.F.R. Part 455**: The FTC's Used Car Rule requires dealers to post a Buyers Guide in every used car they offer for sale. The Used Car Rule also requires dealers to use Spanish-language versions of the Buyers Guide and to make related contract disclosures in Spanish when they conduct sales in Spanish. The Commission issued a Final Rule that made minor corrections to the Spanish translation of the Buyers Guide. The revised Spanish-language versions took effect in February 2013, but dealers were allowed to use up any remaining supplies of the current Buyers Guide. The revised Spanish translations are enclosed and can be found on the FTC's website at business.ftc.gov.[8] "Fillable" versions of the Buyers Guide in English and Spanish are now available.

- **Red Flags Rule, 16 C.F.R. 681**: The Commission and banking agencies promulgated the Red Flags Rule in 2007. The Red Flag Program Clarification Act of 2010, Pub. L. No. 111-319, narrowed the definition of "creditors" covered by the Rule. The Commission published an Interim Final Rule to implement this legislation in December 2012. 77 Fed. Reg. 72,712. The amendment provided that a creditor is covered only if, in the ordinary course of business, it regularly obtains or uses consumer reports in connection with a credit transaction; furnishes information to consumer reporting agencies in connection with a credit transaction; or advances funds to or on behalf of a person, in certain cases. The comment period closed in February 2013, and the Interim Final Rule became final at that time. The Commission published "Fighting Identity Theft with the Red Flags Rule: A How-To Guide for Business,"[9] which has tips for organizations under the FTC's jurisdiction to determine whether they need to design an identity theft prevention program.

For many years, the FTC has had a highly effective program of providing compliance assistance to small businesses[10] We plan to continue to refine and improve these efforts. If you

---

[8] Please see http://business.ftc.gov/documents/gu%C3%ADa-del-comprador-version-para-llenar and http://business.ftc.gov/documents/gu%C3%ADa-del-comprador-con-notas-sobre-el-formato.

[9] The document is enclosed and is found at: http://www.business.ftc.gov/documents/bus23-fighting-identity-theft-red-flags-rule-how-guide-business.

[10] The Commission also considers the specific and unique circumstances of a case when enforcing business obligations. Section 223 of SBREFA (1996) requires that agencies establish policies to reduce or waive penalties for small entities in appropriate circumstances. In 1997, the Commission issued a small business leniency policy statement that describes factors that may result in reduction or waiver of penalties. *See* 62 Fed. Reg. 16,809 (Apr. 8, 1997) (issuing policy); 62 Fed. Reg. 46,363 (Sept. 2, 1997) (responding to comment received). As such cases arise, the Commission considers these leniency factors whenever a civil penalty may be assessed against a small business.

In addition, and beyond SBREFA requirements, the Commission established corporate leniency policies for violations of the Textile and Wool Rules, 67 Fed. Reg. 71,566 (Dec. 2, 2002), the Funeral Rule (through the Funeral Rule Offender Program), and the Franchise Rule (through the Franchise Rule Alternative Law Enforcement Program) that have helped in fostering a more cooperative, less threatening regulatory environment for small entities. These policies have helped increase overall compliance with

have any questions, please contact Christian S. White, the Deputy General Counsel for Legal Counsel and Small Business Coordinator at the Commission, at (202) 326-2476.

Respectfully,e

/signed/
Edith Ramirez
Chairwoman

Enclosures

cc: The Honorable Mary L. Landrieu
Chairwoman
Committee on Small Business & Entrepreneurship
United States Senate
428A Russell Senate Office Building

---

the rules while minimizing the burden on business of correcting certain minor or inadvertent errors that are not likely to injure consumers.

Complying with COPPA: Frequently Asked Questions

A GUIDE FOR BUSINESS AND PARENTS
AND SMALL ENTITY COMPLIANCE GUIDE
(revised July 2013)

The following FAQs are intended to supplement the compliance materials available on the FTC website. In addition, you may send questions or comments to the FTC staff's COPPA mailbox, CoppaHotLine@ftc.gov . This document represents the views of FTC staff and is not binding on the Commission. To view the Rule and compliance materials, go to the FTC's COPPA page for businesses. This document serves as a small entity compliance guide pursuant to the Small Business Regulatory Enforcement Fairness Act.

Some FAQs refer to a type of document called a Statement of Basis and Purpose. A Statement of Basis and Purpose is a document an agency issues when it promulgates or amends a rule, explaining the rule's provisions and addressing comments received in the rulemaking process. A Statement of Basis and Purpose was issued when the COPPA Rule was promulgated in 1999, and another Statement of Basis and Purpose was issued when the Rule was revised in 2012.

Contents:

A. GENERAL QUESTIONS ABOUT THE COPPA RULE
B. COPPA ENFORCEMENT
C. PRIVACY POLICIES AND DIRECT NOTICES TO PARENTS
D. WEB SITES AND ONLINE SERVICES DIRECTED TO CHILDREN
E. PHOTOS, VIDEOS, AND AUDIO RECORDINGS
F. GEOLOCATION DATA
G. GENERAL AUDIENCE, TEEN, AND MIXED-AUDIENCE SITES OR SERVICES
H. VERIFIABLE PARENTAL CONSENT
I. EXCEPTIONS TO PRIOR PARENTAL CONSENT
J. PARENTAL ACCESS TO CHILDREN'S PERSONAL INFORMATION
K. DISCLOSURE OF INFORMATION TO THIRD PARTIES
L. REQUIREMENT TO LIMIT INFORMATION COLLECTION
M. COPPA AND SCHOOLS
N. COPPA SAFE HARBOR PROGRAMS

A. GENERAL QUESTIONS ABOUT THE COPPA RULE

1. What is the Children's Online Privacy Protection Rule?

Congress enacted the Children's Online Privacy Protection Act (COPPA) in 1998. COPPA required the Federal Trade Commission to issue and enforce regulations concerning children's online privacy. The Commission's original COPPA Rule became effective on April 21, 2000. The Commission issued an amended Rule on December 19, 2012. The amended Rule will become effective on July 1, 2013.

The primary goal of COPPA is to place parents in control over what information is collected from their young children online. The Rule was designed to protect children under age 13 while accounting for the dynamic nature of the Internet.

The Rule applies to operators of commercial websites and online services (including mobile apps) directed to children under 13 that collect, use, or disclose personal information from children, and operators of general audience websites or online services with actual knowledge that they are collecting, using, or disclosing personal information from children under 13. The Rule also applies to websites or online services that have actual knowledge that they are collecting personal information directly from users of another website or online service directed to children. Operators covered by the Rule must:

1. *Post a clear and comprehensive online privacy policy describing their information practices for personal information collected online from children;*
2. *Provide direct notice to parents and obtain verifiable parental consent, with limited exceptions, before collecting personal information online from children;*
3. *Give parents the choice of consenting to the operator's collection and internal use of a child's information, but prohibiting the operator from disclosing that information to third parties (unless disclosure is integral to the site or service, in which case, this must be made clear to parents);*
4. *Provide parents access to their child's personal information to review and/or have the information deleted;*
5. *Give parents the opportunity to prevent further use or online collection of a child's personal information;*
6. *Maintain the confidentiality, security, and integrity of information they collect from children, including by taking reasonable steps to release such information only to parties capable of maintaining its confidentiality and security; and*
7. *Retain personal information collected online from a child for only as long as is necessary to fulfill the purpose for which it was collected and delete the information using reasonable measures to protect against its unauthorized access or use.*

2. Who is covered by COPPA?

The Rule applies to operators of commercial websites and online services (including mobile apps) directed to children under 13 that collect, use, or disclose personal information from children. It also applies to operators of general audience websites or online services with actual knowledge that they are collecting, using, or disclosing personal information from children under 13. The Rule also applies to websites or online services that have actual knowledge that they are collecting personal information directly from users of another website or online service directed to children.

3. What is Personal Information?

The amended Rule defines personal information to include:

- First and last name;
- A home or other physical address including street name and name of a city or town;
- Online contact information;
- A screen or user name that functions as online contact information;
- A telephone number;
- A social security number;
- A persistent identifier that can be used to recognize a user over time and across different websites or online services;
- A photograph, video, or audio file, where such file contains a child's image or voice;
- Geolocation information sufficient to identify street name and name of a city or town; or
- Information concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier described above.

4. When does the amended Rule go into effect? What should I do about information I collected from children prior to the effective date that was not considered personal under the original Rule but now is considered personal information under the amended Rule?

The amended Rule, which goes into effect on July 1, 2013, added four new categories of information to the definition of personal information. The amended Rule of course applies to any personal information that is collected after the effective date of the Rule. Below we address, for each new category of personal information, an operator's obligations regarding use or disclosure of previously collected information that will be deemed personal information once the amended Rule goes into effect:

- If you have collected **geolocation information** and have not obtained parental consent, you must do so immediately. Although geolocation information is now a stand-alone category within the definition of personal information, the Commission has made clear that this was simply a clarification of the 1999 Rule. The definition of personal information from the 1999 Rule already covered any geolocation information that provides information precise enough to identify the name of a street and city or town. Therefore, operators are required to obtain parental consent prior to collecting such geolocation information, regardless of when such data is collected.

- If you have collected **photos or videos containing a child's image or audio files with a child's voice from a child** prior to the effective date of the amended Rule, you do not need to obtain parental consent. This is consistent with the Commission's statement contained in the 1999 Statement of Basis and Purpose for the COPPA Rule that operators need not seek parental consent for information collected prior to the effective date of the Rule. However, as a best practice, staff recommends that entities either discontinue the use or disclosure of such information after the effective date of the amended Rule or, if possible, obtain parental consent.

- Under the original Rule, a **screen or user name** was only considered personal information if it revealed an individual's email address. Under the amended Rule, a screen or user name is personal information where it functions in the same manner as online contact information, which includes not only an email address, but any other "substantially similar identifier that permits direct contact with a person online." As with photos, videos, and audio, any newly-covered screen or user name collected prior to the effective date of the amended Rule is not covered by COPPA, although we encourage you as a best practice to obtain parental consent if possible. A previously-collected screen or user name is covered, however, if the operator associates new information with it after the effective date of the amended Rule.

- **Persistent identifiers** were covered by the original Rule only where they were combined with individually identifiable information. Under the amended Rule, a persistent identifier is covered where it can be used to recognize a user over time and across different websites or online services. Consistent with the above, operators need not seek parental consent for these newly-covered persistent identifiers if they were collected prior to the effective date of the Rule. However, if after the effective date of the amended Rule an operator continues to collect, or associates new information with, such a persistent identifier, such as information about a child's activities on its website or online service, this collection of information about the child's activities triggers COPPA. In this situation, the operator is required to obtain prior parental consent unless such collection falls under an exception, such as for support for the internal operations of the website or online service.

5. I don't collect any of the newly-covered types of personal information. Other than the changes to the definition of personal information, in what ways is the new Rule different?

As discussed in additional FAQs below, the amendments to the Rule help to ensure that COPPA continues to meet its originally stated goals to minimize the collection of personal information from children and create a safer, more secure online experience for them, even as online technologies, and children's uses of such technologies, evolve. The final Rule amendments, among other things:

- Modify the definition of "operator" to make clear that the Rule covers an operator of a child-directed site or service where it integrates outside services, such as plug-ins or advertising networks, that collect personal information from its visitors. The definition of "Web site or online service directed to children" was also amended to clarify that the Rule covers a plug-in or ad network when it has actual knowledge that it is collecting personal information through a child-directed Web site or online service and to allow a subset of child-directed sites and services to differentiate among users;
- Streamline and clarify the direct notice requirements to ensure that key information is presented to parents in a succinct ''just-in-time'' notice;
- Expand the non-exhaustive list of acceptable methods for obtaining prior verifiable parental consent;
- Create new exceptions to the Rule's notice and consent requirements;
- Strengthen data security protections;
- Require reasonable data retention and deletion procedures;
- Strengthen the Commission's oversight of self-regulatory safe harbor programs; and
- Institute voluntary pre-approval mechanisms for new consent methods and for activities that support the internal operations of a Web site or online service.

6. Where can I find information about COPPA?

The FTC has a comprehensive Web site, www.ftc.gov, which provides information to the public on a variety of agency activities. Clicking on the Privacy & Security link in the Featured Topics section of the FTC's home page will take you to the Privacy and Security portion of the FTC's Business Center. Clicking on the link labeled Children's Privacy will take you to the Children's Privacy section, which also is accessible by cutting and pasting the following link into a web browser: http://business.ftc.gov/privacy-and-security/children's-privacy. The Children's Privacy section includes a variety of materials regarding COPPA, including all proposed and final Rules, public comments received by the Commission in the course of its rulemakings, guides for businesses, parents, and teachers, information about the Commission-approved COPPA safe harbor programs, and FTC cases brought to enforce COPPA. Many of the educational materials on the FTC Web site also are available in hard copy free of charge by calling the FTC Consumer Response Center's toll free number at (877) FTC-HELP.

7. What should I do if I have questions about the COPPA Rule?

The first thing you should do is read the FTC's Children's Privacy guidance materials. If, after reviewing the FTC's online materials, you continue to have specific COPPA questions, please send an email to our COPPA hotline at CoppaHotLine@ftc.gov .

8. What should I do if I have a complaint about someone violating the COPPA Rule?

You may fill out a complaint form online at Consumer Complaint? Report it to the FTC. You also may call our toll free telephone number, (877) FTC-HELP, to submit your complaint to a live operator.

9. I know that COPPA does not just apply to Web sites, but also to "online services." What types of online services does COPPA apply to?

COPPA applies to personal information collected online by operators of both Web sites and online services. The term "online service" broadly covers any service available over the Internet, or that connects to the Internet or a wide-area network. Examples of online services include services that allow users to play network-connected games, engage in social networking activities, purchase goods or services online, receive online advertisements, or interact with other online content or services. Mobile applications that connect to the Internet, Internet-enabled gaming platforms, voice-over-Internet protocol services, and Internet-enabled location-based services also are online services covered by COPPA.

10. Does COPPA apply to information *about* children collected online from parents or other adults?

No. COPPA only applies to personal information collected online *from* children, including personal information about themselves, their parents, friends, or other persons. However, the Commission's 1999 Statement of Basis and Purpose notes that the Commission expects that operators will keep confidential *any* information obtained from parents in the course of obtaining parental consent or providing for parental access pursuant to COPPA. *See* 64 Fed. Reg. 59888, 59902 n.213.

11. Why does COPPA apply only to children under 13? What about protecting the online privacy of teens?

In enacting the Children's Online Privacy Protection Act, Congress determined to apply the statute's protections only to children under 13, recognizing that younger children are particularly vulnerable to overreaching by marketers and may not understand the safety and privacy issues created by the online collection of personal information.

Although COPPA does not apply to teenagers, the FTC is concerned about teen privacy and does believe that strong, more flexible, protections may be appropriate for this age group. *See* FTC Report: Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers (Mar. 2012), at 29, 60. The FTC also has issued a number of guidance documents for teens and their parents. These educational materials are available at www.OnguardOnline.gov.

12. I know the COPPA Rule is triggered by the collection of personal information from children, but the information I collect at my site or service is voluntary, not mandatory. Does COPPA still apply?

Yes. The Rule governs the online collection of personal information from children by a covered operator, even if children volunteer the information or are not required by the operator to input the information to participate on the Web site or service. The Rule also covers operators that allow children publicly to post personal information. Finally, as the FTC made clear in the amended Rule, the passive tracking of children's personal information through a persistent identifier, and not just its active collection, also is covered by COPPA. *See* 16 C.F.R. § 312.2 (definition of "collection").

13. Will the COPPA Rule keep my child from accessing pornography?

No. COPPA is meant to give parents control over the online collection, use, or disclosure of personal information from children, and was not designed to protect children from viewing particular types of content wherever they might go online. If you are concerned about your children accessing online pornography or other inappropriate materials, you may want to consider a filtering program or an Internet Service Provider that offers tools to help screen out or restrict access to such material. Information about such tools is available at organizations such as www.getnetwise.org and www.staysafeonline.org, and from manufacturers of several operating systems.

14. Will the amended COPPA Rule prevent children from lying about their age to register for general audience sites or online services whose terms of service prohibit their participation?

No. COPPA covers operators of general audience Web sites or online services only where such operators have actual knowledge that a child under age 13 is the person providing personal information. The Rule does not require operators to ask the age of visitors. However, an operator of a general audience site or service that chooses to screen its users for age in a neutral fashion may rely on the age information its users enter, even if that age information is not accurate. In some circumstances, this may mean that children are able to register on a site or service in violation of the operator's Terms of Service. If, however, the operator later determines that a particular user is a child under age 13, COPPA's notice and parental consent requirements will be triggered.

B. COPPA ENFORCEMENT

1. How does the FTC enforce the Rule?

Information about the FTC's COPPA enforcement actions can be found by clicking on the Case Highlights link in the FTC's Business Center. Parents, consumer groups, industry members, and others that believe an operator is violating COPPA may submit complaints to the FTC through the FTC's Web site, www.ftc.gov, or toll free number, (877) FTC-HELP.

2. What are the penalties for violating the Rule?

A court can hold operators who violate the Rule liable for civil penalties of up to $16,000 per violation. The amount of civil penalties a court assesses may turn on a number of factors, including the egregiousness of the violations, whether the operator has previously violated the Rule, the number of children involved, the amount and type of personal information collected, how the information was used, whether it was shared with third parties, and the size of the company. Information about the FTC's COPPA enforcement actions, including the amounts of civil penalties obtained, can be found by clicking on the Case Highlights link in the FTC's Business Center.

3. Can the states or other federal government agencies enforce COPPA?

Yes. COPPA gives states and certain federal agencies authority to enforce compliance with respect to entities over which they have jurisdiction. In the past, Texas and New Jersey have brought COPPA enforcement actions. *See* https://www.oag.state.tx.us/oagnews/release.php?id=2288 (Dec. 2007), and http://www.nj.gov/oag/newsreleases12/pr20120606a.html (June 2012). In addition, certain federal agencies, such as the Office of the Comptroller of the Currency and the Department of Transportation, are responsible for handling COPPA compliance for the specific industries they regulate.

4. What should I do if my Web site or app does not comply with the Rule?

First, until you get your Web site or online service into compliance, you must stop collecting, disclosing, or using personal information from children under age 13.

Second, carefully review your information practices and your online privacy policy. In conducting your review, look closely at what information you collect, how you collect it, how you use it, whether the information is necessary for the activities on your site or online service, whether you have adequate mechanisms for providing parents with notice and obtaining verifiable consent, whether you have adequate methods for parents to review and delete their children's information, and whether you employ adequate data security, retention, and deletion practices.

Educational materials aimed at operators of Web sites and online services are available in the Children's Privacy Section of the FTC's Business Center. *See also* Marketing Your Mobile App: Get it Right From the Start. These materials can provide you with helpful guidance. You might also choose to consult with one of the Commission-approved COPPA Safe Harbor Programs or seek the advice of counsel.

5. Are Web sites and online services operated by nonprofit organizations subject to the Rule?

COPPA expressly states that the law applies to commercial Web sites and online services and not to nonprofit entities that otherwise would be exempt from coverage under Section 5 of the FTC Act. In general, because many types of nonprofit entities are not subject to Section 5 of the FTC Act, these entities are not subject to the Rule. However, nonprofit entities that operate for the profit of their commercial members may be subject to the Rule. *See FTC v. California Dental Association*, 526 U.S. 756 (1999). Although nonprofit entities generally are not subject to COPPA, the FTC encourages such entities to post privacy policies online and to provide COPPA's protections to their child visitors.

6. Does COPPA apply to Web sites and online services operated by the Federal Government?

As a matter of federal policy, all Web sites and online services operated by the Federal Government and contractors operating on behalf of federal agencies must comply with the standards set forth in COPPA. *See* OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (Sept. 2003).

7. The Internet is a global medium. Do Web sites and online services developed and run abroad have to comply with the Rule?

Foreign-based Web sites and online services must comply with COPPA if they are directed to children in the United States, or if they knowingly collect personal information from children in the U.S. The law's definition of "operator" includes foreign-based Web sites and online services that are involved in commerce in the United States or its territories. As a related matter, U.S.-based sites and services that collect information from foreign children also are subject to COPPA.

C. PRIVACY POLICIES AND DIRECT NOTICES TO PARENTS

1. My child-directed Web site does not collect any personal information. Do I still need to post a privacy policy online?

COPPA applies only to those Web sites and online services that collect, use, or disclose personal information from children. However, the FTC recommends that all Web sites and online services – particularly those directed to children – post privacy policies online so visitors can easily learn about the operator's information practices. *See* Mobile Apps for Kids: Disclosures Still Not Making the Grade (Dec. 2012) and Mobile Apps for Kids: Current Privacy Disclosures are Dis*app*ointing (Feb. 2012).

2. What information must I include in my online privacy policy?

Section 312.4(d) of the amended Rule identifies the information that must be disclosed in your online privacy policy. While the original Rule required operators to provide extensive categories of information in their online privacy notices, the amended Rule now takes a shorter, more streamlined approach to cover the information collection and use practices most critical to parents. Under the amended Rule, the online notice must state the following three categories of information:

- The name, address, telephone number, and email address of all operators collecting or maintaining personal information through the site or service (or, after listing all such operators, provide the contact information for one that will handle all inquiries from parents);
- A description of what information the operator collects from children, including whether the operator enables children to make their personal information publicly available, how the operator uses such information, and the operator's disclosure practices for such information; and
- That the parent can review or have deleted the child's personal information and refuse to permit its further collection or use, and state the procedures for doing so. See 16 C.F.R. § 312.4(d) ("notice on the Web site or online service").

By streamlining the Rule's online notice requirements, the Commission hopes to encourage operators to provide clear, concise descriptions of their information practices, which may have the added benefit of being easier to read on smaller screens (e.g., those on smartphones or other Internet-enabled mobile devices).

3. May I include promotional materials in my privacy policy?

No. The Rule requires that privacy policies must be "clearly and understandably written, complete, and must contain no unrelated, confusing, or contradictory materials." *See* 16 C.F.R. § 312.4(a) ("General principles of notice").

4. I already have a privacy policy for my children's app. Do I have to change it to comply with the amended COPPA Rule?

It depends. The amended Rule expands the types of information that are considered "personal." *See* 16 C.F.R. § 312.2 (definition of personal information). Therefore, you should examine your information collection practices to determine whether you are collecting information from children that is now considered personal under the Rule, and that now may require you to notify parents and obtain their consent. In addition, you should review the amended Rule's requirements for the form and content of privacy notices to make sure that your direct notices (*see* FAQ C.11 below) and online privacy policies comply (*see* FAQ C.2 above). *See* 16 C.F.R. § 312.4(b) and (d).

5. Do I have to list the names and contact information of all the operators collecting information at my Web site? This will make my online privacy policy very long and confusing.

The amended Rule retains the requirement that, if there are multiple operators collecting information through your site (including via plug-ins), you may list the name, address, phone number, and email address of one operator who will respond to all inquiries from parents regarding all of the operators' privacy policies and use of children's information, as long as the names of all the operators are also listed in this online notice. *See* 16 C.F.R. § 312.4(d)(1). If you wish to keep your online privacy policy simple, you may include a clear and prominent link in the privacy policy to the complete list of operators, as opposed to listing every operator in the policy itself. You must ensure, however, that your privacy policy signals parents to, and enables them easily to access, this list of operators. *See* .com Disclosures: How to Make Effective Disclosures in Digital Advertising (Mar. 2013), at ii.

6. Do I have to disclose in my privacy policy and direct notices to parents the collection of "cookies," "GUIDs," "IP addresses," or other passive information collection technologies on or through my site?

The amended Rule defines "personal information" to include identifiers, such as a customer number held in a cookie, an IP address, a processor or device serial number, or a unique device identifier that can be used to recognize a user over time and across different Web sites or online services, even where such identifier is not paired with other items of personal information. Therefore, you will need to disclose in your privacy policy (*see* FAQ C.2), and in your direct notice to parents (*see* FAQ C.11), your collection, use or disclosure of such persistent identifiers unless (1) you collect no other "personal information," and (2) such persistent identifiers are collected on or through your site or service solely for the purpose of providing "support for the internal operations" of your site or service. For more detailed information about activities considered support for internal operations, *see* FAQs I.5-8, below.

7. Where should I post links to my privacy policy?

The amended Rule requires that the operator post a clearly and prominently labeled link to the online privacy policy on the home or landing page or screen of the Web site or online service, and at each area of the site or service where personal information is collected from children. This link must be in close proximity to the requests for information in each such area. 16 C.F.R. § 312.4(d).

In addition, an operator of a general audience Web site or online service that has a separate children's area must post a link to its notice of information practices with regard to children on the home or landing page or screen of the children's area. *See* 16 C.F.R. § 312.4(d).

8. Is it okay for the link to my privacy policy to be located at the bottom of the home page of my Web site?

The amended Rule states that the "operator must post a prominent and clearly labeled link to an online notice of its information practices with regard to children on the home or landing page or screen of its Web site or online service, *and,* at each area of the Web site or online service where personal information is collected from children." 16 C.F.R. § 312.4(d). In the 1999 Statement of Basis and Purpose, the Commission explained that "'clear and prominent' means that the link must stand out and be noticeable to the site's visitors through use, for example, of a larger font size in a different color on a contrasting background. The Commission does not consider 'clear and prominent' a link that is in small print at the bottom of the home page, or a link that is indistinguishable from a number of other, adjacent links." *See* 64 Fed. Reg. 59888, 59894. A link that is at the bottom of the page *may* be acceptable if the manner in which it is presented makes it clear and prominent.

9. I have an app directed to children. Do I need to make sure that my privacy policy is included in the app store, at the point of purchase or download?

The amended Rule does not mandate that a privacy policy be posted at the point of purchase; rather, the Rule requires that it be posted on the home or landing screen. However, there is a substantial benefit in providing greater transparency about the data practices and interactive features of child-directed apps at the point of purchase and we encourage it as a best practice. In fact, the FTC Staff Report, Mobile Apps for Kids: Disclosures Still Not Making the Grade (Dec. 2012) notes that "information provided prior to download is most useful in parents' decision-making since, once an app is downloaded, the parent already may have paid for the app..." *See* p. 7. Further, if a child-directed app were designed to collect personal information as soon as it is downloaded, it would be necessary to provide the direct notice and obtain verifiable consent at the point of purchase or to insert a landing page where a parent can receive notice and give consent before the download is complete.

10. I operate a general audience Web site that contains a specific children's section. May I post a single privacy policy for the entire site that combines information about my children's and general information practices, or must I have a separate privacy policy for children's data?

In the 1999 Statement of Basis and Purpose, the Commission noted that "operators are free to combine the privacy policies into one document, as long as the link for the children's policy takes visitors directly to the point in the document where the operator's policies with respect to children are discussed, or it is clearly disclosed at the top of the notice that there is a specific section discussing the operator's information practices with regard to children." *See* 64 Fed. Reg. 59888, 59894 n.98. This advice remains in effect under the amended Rule. Operators should also ensure that the link for the children's portion of the privacy policy appears on the home page or screen of the children's area of the site or service, and at each area where personal information is collected from children. *See* 16 C.F.R. § 312.4(d).

11. I know that the amended Rule made some changes to the direct notice that must be sent to parents before I collect personal information from children. What are those changes?

The Rule requires operators to make reasonable efforts, taking into account available technology, to ensure that a parent of a child receives direct notice of the operator's practices with regard to the collection, use, or disclosure of personal information from children, including notice of any material changes to practices to which the parent previously consented. The amended Rule significantly changed the format and content of the information that must be included in an operator's direct notice to parents. The Rule now provides a very detailed roadmap of what information must be included in your direct notice depending upon what personal information is collected and for what purposes.

There are four instances where a direct notice is required or appropriate under the Rule:

1. Where an operator seeks to obtain a parent's verifiable consent prior to the collection, use, or disclosure of a child's personal information. In this case, the direct notice must:
    - State that the operator has collected the parent's online contact information from the child, and, if such is the case, the name of the child or the parent, in order to obtain the parent's consent;
    - State that the parent's consent is required for the collection, use, or disclosure of such information, and that the operator will not collect, use, or disclose any personal information from the child if the parent does not provide such consent;
    - Set forth the additional items of personal information the operator intends to collect from the child, or the potential opportunities for the disclosure of personal information, should the parent provide consent;
    - Contain a hyperlink to the operator's online notice of its information practices (i.e., its privacy policy);
    - Provide the means by which the parent can provide verifiable consent to the collection, use, and disclosure of the information; and
    - State that if the parent does not provide consent within a reasonable time from the date the direct notice was sent, the operator will delete the parent's online contact information from its records. *See* 16 C.F.R. § 312.4(c)(1).

2. Where an operator voluntarily seeks to provide notice to a parent of a child's online activities that do not involve the collection, use or disclosure of personal information. In this case, the direct notice must:
    - State that the operator has collected the parent's online contact information from the child in order to provide notice to, and subsequently update the parent about, a child's participation in a Web site or online service that does not otherwise collect, use, or disclose children's personal information;

State that the parent's online contact information will not be used or disclosed for any other purpose;

- State that the parent may refuse to permit the child's participation in the Web site or online service and may require the deletion of the parent's online contact information, and how the parent can do so; and
- Provide a hyperlink to the operator's online notice of its information practices. *See* 16 C.F.R. § 312.4(c)(2).

3. Where an operator intends to communicate with the child multiple times via the child's online contact information and collects no other information. In this case, the direct notice must:
    - State that the operator has collected the child's online contact information from the child in order to provide multiple online communications to the child;
    - State that the operator has collected the parent's online contact information from the child in order to notify the parent that the child has registered to receive multiple online communications from the operator;
    - State that the online contact information collected from the child will not be used for any other purpose, disclosed, or combined with any other information collected from the child;
    - State that the parent may refuse to permit further contact with the child and require the deletion of the parent's and child's online contact information, and how the parent can do so;
    - State that if the parent fails to respond to this direct notice, the operator may use the online contact information collected from the child for the purpose stated in the direct notice; and
    - Provide a hyperlink to the operator's online notice of its information practices. *See* 16 C.F.R. § 312.4(c)(3).

4. Where the operator's purpose for collecting a child's and a parent's name and online contact information is to protect a child's safety and the information is not used or disclosed for any other purpose. In this case, the direct notice must:
    - State that the operator has collected the name and the online contact information of the child and the parent in order to protect the safety of a child;
    - State that the information will not be used or disclosed for any purpose unrelated to the child's safety;
    - State that the parent may refuse to permit the use, and require the deletion, of the information collected, and how the parent can do so;
    - State that if the parent fails to respond to this direct notice, the operator may use the information for the purpose stated in the direct notice; and
    - Provide a hyperlink to the operator's online notice of its information practices. *See* 16 C.F.R. § 312.4(c)(4).

12. When I send a direct notice to parents, may I send them a simple email containing a link to my online privacy policy?

No. As described in FAQ C.11 above, the amended Rule makes clear that the direct notice to parents must contain certain key information within the four corners of the notice itself, depending on the purpose for which the information is being collected. Therefore, you may not simply link to a separate online notice. Note, however, that in addition to the key information, the amended Rule requires that each direct notice you send also contain a link to your online privacy policy. The intention of these changes is to help ensure that the direct notice functions as an effective "just-in-time" message to parents about an operator's information practices, while also directing parents online to view any additional information contained in the operator's online notice.

13. I have an app directed to children. At what point in the download process should I send parents my direct notice?

Unless one of the limited exceptions applies (*see* FAQ H.2), the Rule requires that you send parents the direct notice prior to the collection of any personal information from the child. The limited exception to this is that you may collect the parent's online contact information for the sole purpose of sending the parent the direct notice. Alternatively, you may provide the direct notice to the parent through other means, such as through the device onto which the app is downloaded, if the mechanisms both (1) provide such notice and obtain the parent's consent before any collection of personal information and (2) are reasonably designed to ensure that it is the parent who receives the notice and provides the consent.

D. WEB SITES AND ONLINE SERVICES DIRECTED TO CHILDREN

1. COPPA applies to Web sites or online services that are "directed to children." What determines whether or not a Web site or online service is directed to children?

The amended Rule sets out a number of factors for determining whether a Web site or online service is directed to children. These include subject matter of the site or service, its visual content, the use of animated characters or child-oriented activities and incentives, music or other audio content, age of models, presence of child celebrities or celebrities who appeal to children, language or other characteristics of the Web site or online service, or whether advertising promoting or appearing on the Web site or online service is directed to children. The Rule also states that the Commission will consider competent and reliable empirical evidence regarding audience composition, as well as evidence regarding the intended audience of the site or service. *See* 16 C.F.R. § 312.2 (definition of "Web site or online

service directed to children," paragraph (1)).

As described in FAQ D.5 below, the amended Rule also considers a Web site or online service to be "directed to children" where it has actual knowledge that it is collecting personal information directly from users of another Web site or online service that is directed to children. *See* 16 C.F.R. § 312.2 (definition of "Web site or online service directed to children," paragraph (2)).

2. I run a child-directed app. I would like to screen users so that I only have to get parental consent from children under age 13, not from everyone who uses the app. May I?

It depends. Because of its very nature, in most instances, a Web site or online service (such as an app) directed to children must treat all visitors as children and provide COPPA's protections to every such visitor. This means that for the most part, a Web site or online service directed to children may not screen users for age.

However, the amended Rule provides for a narrow exception for a site or service that may be directed to children under the criteria set forth in FAQ D.1 above, but that does not target children as its *primary* audience. For instance, a child-directed site may target children under age 13, as well as parents or younger teens. An operator of a site or service meeting this standard may age-screen its users if it: (1) does not collect personal information from any visitor prior to collecting age information, and (2) prevents the collection, use, or disclosure of personal information from visitors who identify themselves as under age 13 without first complying with the amended Rule's notice and parental consent provisions. *See* 16 C.F.R. § 312.2 (definition of "Web site or online service directed to children," paragraph (3)). Importantly, as an operator of a Web site or online service directed to children, you may not block children from participating in the Web site or online service (*see* FAQ D.4 below).

3. What evidence would I need to demonstrate whether children under age 13 are or are not the "primary target audience" for my Web site?

As the operator, you should carefully analyze who your intended audience is, the actual audience, and in many instances, the likely audience for your site or service. In making these determinations, you should keep in mind the factors for a "Web site or online service directed to children" contained in paragraph (1) of 16 C.F.R. § 312.2. *See* FAQ D.1 above. You may also get a better sense of your site or service once it has been in operation, and may need to make some changes accordingly.

4. I run a site that I believe may fall within the FTC's sub-category of a Web site directed to children but where it is acceptable to age-screen users. Can I age-screen and completely block users who identify as being under age 13 from participating in any aspect of my site?

No. If your site falls within the definition of a "Web site or online service directed to children" as set forth in paragraph (1) of 16 C.F.R. § 312.2, then you may not block children from participating altogether, even if you do not intend children to be your primary target audience. Instead, what the amended Rule now permits you to do is to use an age screen in order to differentiate between your child and non-child users. You may decide to offer different activities, or functions, to your users depending upon age, but you may not altogether prohibit children from participating in a child-directed site or service.

5. [Now at FAQ D.10]

6. Am I required to inform third parties that my Web site or online service is directed to children? Even if I am not required to do so, how can I do this? If I signal the nature of my site or service, will this protect me from liability under COPPA?

The amended Rule does not require you to inform third parties of the child-directed nature of your site or service, and doing so, without more, will not relieve you of your obligations under COPPA. Remember, you are responsible for the collection of personal information from your users, no matter who is doing the collection; therefore, you will need to do more than simply identify yourself to third parties. As a child-directed property, absent an exception under the amended Rule (*see* FAQ H.2 below), you must: (1) not collect or allow any other entity to collect personal information from your visitors; or (2) provide notice and obtain prior parental consent before collecting or allowing any entity to collect personal information from your visitors, as well as provide all of the other COPPA protections. In addition, Commission staff recommends that operators of child-directed Web sites or services signal their status to third parties and you may arrange with the third party collecting the personal information to provide adequate COPPA protections.

7. I want to run ads on my child-directed Web sites and apps. What do I need to know to make sure that I am complying with COPPA?

There are a number of questions you must find answers to before you enter into an arrangement with any entity to serve advertising to run on your child-directed sites and services. These include:

- Is there a way to control the type of advertising that appears on the sites and services? (*e.g.*, can you stipulate and contract only for contextual advertising, and can you prohibit behavioral advertising or retargeting?)
- What categories of information will be collected from users on the sites and services in connection with the ads they are served? Will persistent identifiers be collected for purposes other than support for internal operations? Will geolocation information be collected in connection with the ads served?

You should make informed decisions before you permit advertising to run on your sites and services. Depending on

what advertising choices you make, you may be required to notify parents in your online privacy policies and in a direct notice, and obtain verifiable parental consent, before you permit advertising to occur. Remember that the amended Rule holds you liable for the collection of information that occurs on or through your sites and services, even if you yourself do not engage in such collection.

8. I have no idea what information the third parties whose content I have embedded in my kids' app might collect from my users. Do I need to know this information?

Yes. As the operator of a child-directed app, you must conduct an inquiry into the information collection practices of every third party that can collect information via your app. You need to determine each third party's information collection practices so that you can make an informed decision as to whether its presence on your app will require you to give parents notice and obtain their consent prior to their collection of personal information from children. *See* FAQ D.6 above.

9. I operate a child-directed app that allows kids to make paintings. I don't collect the paintings — they rest on the device — but the app includes buttons for popular email and social media providers that kids can click on within the app. The buttons open the email program or social network, populate it with the painting, and allow the child to share it along with a message. I don't collect or share any other personal information through the app. Do I have to seek verifiable parental consent?

Yes. The COPPA rule defines "collection" to include requesting, prompting, or encouraging a child to submit personal information online, and enabling a child to make personal information publicly available in identifiable form. In addition, under the COPPA Rule, "disclosure" includes making a child's personal information publicly available in identifiable form through an email service or other means, such as a social network. You must get verifiable parental consent before enabling children to share personal information in this manner, even through third parties on your app. This is true unless an exception applies. (See Section I, Exceptions to Prior Parental Consent). However, in the situation you describe — where a child can email a painting and a message or post content on his or her social networking page through your app — no exception applies.

10. I operate an advertising network service. Under what circumstances will I be held to have "actual knowledge" that I have collected personal information directly from users of another Web site or online service directed to children?

The circumstances under which you will be deemed to have acquired "actual knowledge" that you have collected personal information directly from users of a child-directed site or service will depend a lot on the particular facts of your situation. In the 2012 Statement of Basis and Purpose, the Commission set forth two cases where it believes that the actual knowledge standard will likely be met:

1. where a child-directed content provider (which is strictly liable for any collection) directly communicates the child-directed nature of its content to you, the ad network; or

2. where a representative of your ad network recognizes the child-directed nature of the content.

Under the first scenario, any direct communications that the child-directed provider has with you that indicate the child-directed nature of its content would give rise to actual knowledge. In addition, if a formal industry standard or convention is developed through which a site or service could signal its child-directed status to you, that would give rise to actual knowledge. Under the second scenario, whether a particular individual can obtain actual knowledge on behalf of your business depends on the facts. Prominently disclosing on your site or service methods by which individuals can contact your business with COPPA information – such as: 1) contact information for designated individuals, 2) a specific phone number, and/or 3) an online form or email address – will reduce the likelihood that you would be deemed to have gained actual knowledge through other employees. (See also FAQ D.12 below).

11. I operate an ad network. I receive a list of Web sites from a parents' organization, advocacy group or someone else, which says that the Web sites are child-directed. Does this give me actual knowledge of the child-directed nature of these sites?

It's unlikely the receipt of a list of purportedly child-directed Web sites alone would constitute actual knowledge. You would have no duty to investigate. It's possible, however, that you will receive screenshots or other forms of concrete information that do give you actual knowledge that the Web site is directed at children. If you receive information and are uncertain whether the site is child-directed, you may ordinarily rely on a specific affirmative representation from the Web site operator that its content is not child-directed. For this purpose, a Web site operator would not be deemed to have provided a specific affirmative representation if it merely accepts a standard provision in your Terms of Service stating that, by incorporating your code, the first party agrees that it is not child directed.

12. I operate an ad network and am considering participating in a system in which first-party sites could signal their child-directed status to me, such as by explicit signaling from the embedding webpage to ad networks. I understand that I would have "actual knowledge" if I collect information from users on a first-party site that has signaled its child-directed status. Are there any benefits to me if I participate in such a system?

Such a system could provide more certainty for you. If the system requires the first-party site to affirmatively certify whether it is "child-directed" or "not child-directed," and the site signals that it is "not child-directed," you may ordinarily rely on such a representation. Such reliance is advisable, however, only if first parties affirmatively signal that their sites or services are "not child-directed." You could not set that option for them as the default.

Remember, though, that you may still be faced with screenshots or other concrete information that gives you actual knowledge of the child-directed nature of the Web site despite a contradictory representation by the site. If, however, such information is inconclusive, you may ordinarily continue to rely on a specific affirmative representation made through a system that meets the criteria above.

E. PHOTOS, VIDEOS, AND AUDIO RECORDINGS

1. I run a moderated Web site that is directed to children and I prescreen all children's submissions in order to delete personal information before postings go live. Do I have to get parental consent if I allow children to post photos of themselves but no other personal information?

Yes. The amended Rule considers photos, videos, and audio recordings that contain a child's image or voice to be personal information. This means that operators covered by COPPA must either (i) prescreen and delete from children's submissions any photos, videos, or audio recordings of themselves or other children or (ii), first give parents notice and obtain their consent prior to permitting children to upload any photos, videos, or audio recordings of themselves or other children.

2. I want to offer a child-directed app. The app would allow children to upload pictures of their favorite pets or places. I do not ask children to provide their email addresses or their names, or really any personal information for that matter. How does COPPA apply to me?

COPPA applies to photos, videos, and audio files that contain children's images or voices. It also applies to geolocation data contained in these files sufficient to identify street name and name of city or town. Finally, it applies to any persistent identifiers collected via the children's upload of their photos. Therefore, in order to offer an app without parental notice and consent, the operator must take the following steps

1. Pre-screen the children's photos in order to delete any that depict images of children or to delete the applicable portion of the photo, if possible. The operator must also remove any other personal information, for example, geolocation metadata, contained in the photos prior to posting them through the app. Note that if an operator does not pre-screen, then it may be subject to civil penalties under COPPA if any personal information is collected from children without the operator first notifying parents and obtaining their consent; and

2. Ensure that any persistent identifiers are used only to support the internal operations of the app (as that term is defined in the Rule) and are not used or disclosed to contact a specific individual or for any other purpose.

3. Do I have to get parental consent if first I blur images in the children's photos so that you cannot see any facial features when the pictures go live on my site?

An operator of a site directed to children does not need to notify parents or obtain their consent if it blurs the facial features of children in photos before posting them on its Web site. *See* 2012 Statement of Basis and Purpose, 78 Fed. Reg. 3972, 3982 n.123. The same goes for a site that has actual knowledge it has collected the photos from children. Before posting such photos, however, the operator must also remove any other personal information they contain, such as geolocation metadata, and ensure that it is not using or disclosing persistent identifiers collected from children in a manner that violates the amended Rule.

4. Does the amended Rule prohibit adults, such as parents, grandparents, teachers, or coaches from uploading photos of children?

COPPA only covers information collected online from children. It does not cover information collected from adults that may pertain to children. Thus, COPPA is not triggered by an adult uploading photos of children on a general audience site or in the non-child directed portion of a mixed-audience Web site.

However, operators of Web sites or online services that are primarily directed to children (as defined by the Rule) must assume that the person uploading a photo is a child and they must design their systems either to: (1) give notice and obtain prior parental consent, (2) remove any child images and metadata prior to posting, or (3) create a special area for posting by adults, if that is the intention.

5. My app is directed to children. A child can upload photos into the app and manipulate and decorate the photos in different ways, but the app does not transmit any personal information (photos or otherwise) from the child's device. Am I "collecting" personal information because the child is interacting with a photo stored on the device?

No. You are not collecting personal information simply because your app interacts with personal information that is stored on the device and is never transmitted.

F. GEOLOCATION DATA

1. I automatically collect geolocation information from users of my children's app, but I do not use this information for anything. Am I responsible for notifying parents and getting their consent to such collection?

Yes. COPPA covers the collection of geolocation information, not just its use or disclosure.

2. What if I give my users a choice to turn off geolocation information? Do I still have to notify parents and get prior parental consent?

COPPA is designed to notify parents and give them the choice to consent. Therefore, it is not sufficient to provide such notification and choice to the child user of a Web site or service. If the operator intends to collect geolocation information, the operator will be responsible for notifying parents and obtaining their consent prior to such collection.

3. The amended Rule covers "geolocation information sufficient to identify street name and name of city or town." What if my children's app only collects coarse geolocation information, tantamount to collecting a ZIP code but nothing more specific?

COPPA does not require an operator to notify parents and obtain their consent before collecting the type of coarse geolocation services described. However, the operator should be quite certain that, in all instances, the geolocation information it collects is more general than that sufficient to identify street name and name of city or town.

4. The geolocation information I collect through my app provides coordinate numbers. It does not specifically identify a street name and name of city or town. Do I have to notify parents and get their consent in this instance?

COPPA covers the collection of geolocation information "sufficient" to identify street name and name of city or town. It does not require the actual address identification of such information at the time of collection. One example where COPPA would be triggered is where an app takes the user's longitude and latitude coordinates and translates them to a precise location on a map.

G. GENERAL AUDIENCE, TEEN, AND MIXED-AUDIENCE SITES OR SERVICES

1. Am I responsible if children lie about their age during the registration process on my general audience Web site?

The Rule does not require operators of general audience sites to investigate the ages of visitors to their sites or services. *See* 1999 Statement of Basis and Purpose, 64 Fed. Reg. 59888, 59892. However, operators will be held to have acquired actual knowledge of having collected personal information from a child where, for example, they later learn of a child's age or grade from a concerned parent who has learned that his child is participating on the site or service.

2. I have an online service that is intended for teenagers. How does COPPA affect me?

Although you may intend to operate a "teen service," in reality, your site may attract a substantial number of children under 13, and thus may be considered to be a "Web site or online service directed to children" under the Rule. Just as the Commission considers several factors in determining whether a site or service is directed to children, you too should consider your service's subject matter, visual content, character choices, music, and language, among other things. If your service targets children as one of its audiences – even if children are not the primary audience – then your service is "directed to children."

In circumstances where children are not the primary audience of your child-directed service, the amended Rule allows you to employ an age screen in order to provide COPPA's protections to only those visitors who indicate they are under age 13. Note that sites or services directed to children cannot use the age screen to block children under age 13. *See* FAQ D.2 above. Once you identify child visitors, you may choose to:

1. Collect parents' online contact information to provide direct notice in order to obtain parents' consent to your information collection, use and disclosure practices; or
2. Direct child visitors to content that does not involve the collection, use, or disclosure of personal information.

3. Can I block children under 13 from my general audience Web site or online service?

Yes. COPPA does not require you to permit children under age 13 to participate in your general audience Web site or online service, and you may block children from participating if you so choose. By contrast, you may not block children from participating in a Web site or online service that is directed to children as defined by the Rule. *See* FAQ D.2 above.

If you choose to block children under 13 on your general audience site or service, you should take care to design your age screen in a manner that does not encourage children to falsify their ages to gain access to your site or service. Ask age information in a neutral manner at the point at which you invite visitors to provide personal information or to create a user ID.

In designing a neutral age-screening mechanism, you should consider:

- Making sure the data entry point allows users to enter their age accurately. An example of a neutral age-screen would be a system that allows a user freely to enter month, day, and year of birth. A site that includes a drop-down menu that only permits users to enter birth years making them 13 or older, would not be considered a neutral age-screening mechanism since children cannot enter their correct ages on that site.

- Avoiding encouraging children to falsify their age information, for example, by stating that visitors under 13

cannot participate or should ask their parents before participating. In addition, simply including a check box stating, "I am over 12 years old" would not be considered a neutral age-screening mechanism.

In addition, consistent with long standing Commission advice, FTC staff recommends using a cookie to prevent children from back-buttoning to enter a different age. Note that if you ask participants to enter age information, and then you fail either to screen out children under age 13 or to obtain their parents' consent to collecting these children's personal information, you may be liable for violating COPPA. *See, e.g.,* the FTC's COPPA cases against *Path, Inc.*, *Playdom, Inc.* and *Sony BMG Music Entertainment*.

4. I operate a general audience gaming site and do not ask visitors to reveal their ages. I do permit users to submit feedback, comments, or questions by email. What are my responsibilities if I receive a request for an email response from a player who indicates that he is under age 13?

Under the Rule's one-time response exception (16 C.F.R. § 312.5(c)(3)) you are permitted to send a response to the child, via the child's online contact information, without sending notice to the parent or obtaining parental consent. However, you must delete the child's online contact information from your records promptly after you send your response. You may not use the child's online contact information to re-contact the child (or for any other purpose), or disclose the child's online contact information. Note that if you choose not to respond to the child's inquiry, you must still immediately delete the child's personal information from your records. Additionally, such an email may give you actual knowledge that you have collected personal information from a child (*e.g.*, if you had previously collected the child's email address as part of a Web site registration process). In such a circumstance, you would need to take steps to ensure that you are complying with COPPA, such as obtaining parental consent or immediately deleting any personal information collected from the child.

5. I operate a general audience online service and do not ask visitors to reveal their ages. However, I do permit users to create their own blog pages, and my service has a number of online forums.

(a) What happens if a child registers on my service and posts personal information (*e.g.,* on a comments page) but does not reveal his age anywhere?

The COPPA Rule is not triggered in this scenario. The Rule applies to an operator of a general audience Web site if it has actual knowledge that a particular visitor is a child. If a child posts personal information on a general audience site or service but does not reveal his age, and if the operator has no other information that would lead it to know that the visitor is a child, then the operator would not be deemed to have acquired "actual knowledge" under the Rule and would not be subject to the Rule's requirements.

However, even where a child himself has not revealed his age on a site or service, an operator may acquire actual knowledge where it later learns of a child's age – for example, through a report from a concerned parent who has discovered that her child is participating on the site. Where an operator knows that a particular visitor is a child, the operator must either meet COPPA's notice and parental consent requirements or delete the child's information.

(b) What happens if a child posts in a forum and announces her age?

If no one in your organization is aware of the post, then you may not have the requisite actual knowledge under the Rule. However, you may be considered to have actual knowledge where a child announces her age under certain circumstances, for example, if you monitor your posts, if a responsible member of your organization sees the post, or if someone alerts you to the post (*e.g.*, a concerned parent who learns that his child is participating on your site).

H. VERIFIABLE PARENTAL CONSENT

1. When do I have to get verifiable parental consent?

The Rule provides generally that an operator must obtain verifiable parental consent before collecting any personal information from a child, unless the collection fits into one of the Rule's exceptions described in various FAQs herein. *See* 16 C.F.R. § 312.5(c).

2. May I first collect personal information from the child, and then get parental permission to such collection if I do not use the child's information before getting the parent's consent?

As a general rule, operators must get verifiable parental consent before collecting personal information online from children under 13. Certain, limited exceptions let operators collect certain personal information from a child before obtaining parental consent. *See* 16 C.F.R. § 312.5(c). These exceptions include:

- Where the sole purpose of collecting a parent's online contact information is to provide voluntary notice about the child's participation in a Web site or online service that does not otherwise collect, use, or disclose children's personal information. Such information cannot be used or disclosed for any other purpose and the operator must make reasonable efforts, taking into consideration available technology, to provide a parent with appropriate notice;

- Where the sole purpose of collecting online contact information from a child is to respond directly on a one-time basis to a specific request from the child, and where such information is not used to re-contact the child or for any other purpose, is not disclosed, and is deleted by the operator from its records promptly after responding to the child's request;

- Where the purpose of collecting a child's and a parent's online contact information is to respond directly more than once to the child's specific request, and where such information is not used for any other purpose, disclosed, or combined with any other information collected from the child. Here, the operator must provide parents with notice and the means to opt out of allowing the site's future contact of the child. In providing such notice, the operator must make reasonable efforts, taking into consideration available technology, to ensure that the parent receives appropriate notice and will not be deemed to have made reasonable efforts where the notice to the parent was unable to be delivered;

- Where the purpose of collecting a child's and a parent's name and online contact information, is to protect the safety of a child, and where such information is not used or disclosed for any purpose unrelated to the child's safety. Here, the operator must make reasonable efforts, taking into consideration available technology, to provide a parent with appropriate notice;

- Where the purpose of collecting a child's name and online contact information is to:
  - Protect the security or integrity of its Web site or online service;
  - Take precautions against liability;
  - Respond to judicial process; or
  - To the extent permitted under other provisions of law, to provide information to law enforcement agencies or for an investigation on a matter related to public safety;

- Where an operator collects a persistent identifier and no other personal information and such identifier is used for the sole purpose of providing support for the internal operations of the Web site or online service as outlined in FAQ I.5 below; or

- Where a third-party operator has actual knowledge that it has a presence on a child-directed site (*e.g.*, through a social widget or plug-in embedded on the site), it collects a persistent identifier and no other personal information from a visitor of the child-directed site, and the third-party operator's previous affirmative interaction with that user confirmed the user was not a child (*e.g.*, an age-gated registration process).

3. I collect personal information from children who use my online service, but I only use the personal information I collect for internal purposes and I never give it to third parties. Do I still need to get parental consent before collecting that information?

It depends. First, you should determine whether the information you collect falls within one of the amended Rule's limited exceptions to parental consent outlined in FAQ H.2 above. If you fall outside of one of those exceptions, you must notify parents and obtain their consent. However, if you only use the information internally, and do not disclose it to third parties or make it publicly available, then you may obtain parental consent through use of the Rule's "email plus" mechanism, as outlined in FAQ H.4 below. *See* 16 C.F.R. § 312.5(b)(2).

4. How do I get parental consent?

You may use any number of methods to obtain verifiable parental consent, as long as the method you choose is reasonably calculated to ensure that the person providing consent is the child's parent. The Rule sets forth several non-exhaustive options, and you can apply to the FTC for pre-approval of a new consent mechanism, as set out in FAQ H.14 below.

If you are going to disclose children's personal information to third parties, or allow children to make it publicly available (*e.g.*, through a social networking service, online forums, or personal profiles) then you must use a method that is reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent. Such methods include:

- Providing a consent form to be signed by the parent and returned via U.S. mail, fax, or electronic scan (the "print-and-send" method);
- Requiring the parent, in connection with a monetary transaction, to use a credit card, debit card, or other online payment system that provides notification of each discrete transaction to the primary account holder;
- Having the parent call a toll-free telephone number staffed by trained personnel, or have the parent connect to trained personnel via video-conference; or
- Verifying a parent's identity by checking a form of government-issued identification against databases of such information, provided that you promptly delete the parent's identification after completing the verification.

If you are going to use children's personal information only for internal purposes – that is, you will not be disclosing the information to third parties or making it publicly available – then you can use any of the above methods or you can use the "email plus" method of parental consent. "Email plus" allows you to request (in the direct notice sent to the parent's online contact address) that the parent indicate consent in a return message. To properly use the email plus method, you must take an additional confirming step after receiving the parent's message (this is the "plus" factor). The confirming step may be:

- Requesting in your initial message to the parent that the parent include a phone or fax number or mailing address in the reply message, so that you can follow up with a confirming phone call, fax or letter to the parent; or

- After a reasonable time delay, sending another message via the parent's online contact information to confirm consent. In this confirmatory message, you should include all the original information contained in the direct notice, inform the parent that he or she can revoke the consent, and inform the parent how to do so.

5. I would like to get consent by collecting a credit card or debit card number from the parent, but I do not want to engage in a monetary transaction. Is this ok?

No. The amended Rule permits an operator to use a credit card, debit card, or other online payment system as a form of verifiable parental consent, but only if the card or payment system: (1) is used in connection with a monetary transaction, and (2) provides notification of each discrete transaction to the primary account holder. Therefore, use of a credit or debit card, without a monetary transaction, is not an acceptable method of verifiable parental consent.

6. I would like to use a credit card or a government-issued identification as a method of parental consent. I am worried, however, that I will not know whether it is the child's parent or another adult who is submitting identification for consent. Do I need to collect additional information to confirm that, in fact, it is the parent?

No. By providing appropriate notice and obtaining consent in connection with the amended Rule's proper use of a credit card or government identification, the operator will be deemed to fulfill its obligation under the Rule.

7. What do I do if some parents cannot or will not use the consent method I have chosen? For instance, some parents might not have a credit card, or might feel uncomfortable providing government identification information online.

Many operators find it useful to offer a choice of consent methods for those parents who cannot, or will not, use their primary consent mechanism. At the very least, you might consider offering one alternate method that parents might be more comfortable with, such as a print-and-send form.

8. Should I give out passwords or PIN numbers to parents to confirm their identity in any future contact with them?

Once you have notified a parent and obtained verifiable consent, providing a password or a PIN number is a good way to confirm a parent's identity for any future contact you might have with that parent. Remember that if you change your information practices in a material way in the future, you will have to send a new parental notice and obtain an updated consent to the new practices. Obtaining an updated consent may be easier if you have given the parent a password or a PIN number in your initial consent process.

In addition, the Rule requires you to give a parent access to any personal information you have collected from the child. Before you provide that information, you will need to confirm that the person requesting the information is the child's parent. Again, providing the parent a password or a PIN number makes it easier to confirm the parent's identity if the parent requests access to the child's personal information.

9. I know that I must allow parents to consent to my collection and use of their children's information, while giving them the option of prohibiting me from disclosing that information to third parties. Does that mean that if I operate a social networking site, or have chat rooms or message boards, I have to offer the same kind of "choice" about these types of sites as well?

The Rule requires an operator to give parents the option to consent to the collection and use of a child's personal information without consenting to the disclosure of such information to third parties. *See* 16 C.F.R. § 312.5(a)(2). However, an operator must only provide this choice where the disclosure of the information is not inherent in the activity to which the parent is consenting.

You should note that the Rule's definition of "disclosure" is broader than merely "releasing" personal information to third parties. Under the Rule, "disclosure" includes "[m]aking personal information collected by an operator from a child publicly available in identifiable form by any means, including but not limited to a public posting through the Internet, or through a personal home page or screen posted on a Web site or online service; a pen pal service; an electronic mail service; a message board; or a chat room." *See* 16 C.F.R. § 312.2.

In the case of social networking sites, chat rooms, message boards, and other similar online services, sharing personal information is a central feature of the site. Therefore, in these cases, you are not required to give parents the choice to allow you to collect and use their children's personal information, but not disclose it to third parties. However, you must clearly disclose your information collection, use, and disclosure practices in your direct notice and online privacy policy so that parents can make an informed decision about their children's participation in your site or service.

10. As a mobile app operator, can I rely on a parent's app store account to serve as verifiable parental consent if a credit card is attached to that account?

Without more, the collection of a parent's app account number or password is insufficient to fulfill the Rule's notice and consent requirements. In order to meet the Rule's notice requirements, the operator must provide parents with a direct notice outlining the operator's information collection practices. In addition, the Rule requires that the consent mechanism used must be reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent. The mere entry of an app store account number or password, without other indicia of reliability (*e.g.*, knowledge-based authentication questions or verification of government identification), does not provide sufficient assurance that the person entering the account or password information is the parent, and not the child.

11. What types of information can I collect to obtain or confirm parental consent? Can I use a parent's mobile phone number to obtain or confirm parental consent?

The Rule permits you to collect the parent's "online contact information," defined as an email address, an IM user identifier, a VOIP identifier, a video chat user identifier, or other substantially similar identifier. A mobile phone number is not online contact information and therefore cannot be collected from the child as part of the consent initiation process. However, once you have connected with the parent via the parent's online contact information, you may request a parent's mobile phone number in order to further communicate with him or her.

12. How long will "email plus" remain an approved form of parental consent?

The amended Rule identifies email plus as an acceptable method for verifiable parental consent where an operator does not "disclose" children's personal information. The Commission has determined that email-plus shall be permanent, just as are the other approved methods for verifiable parental consent.

13. Can I use a third party to carry out my notice and consent obligations for me?

Yes. For instance, several of the Commission-approved COPPA safe harbor programs offer parental notification and consent systems for operators who are members of their programs. In addition, the Commission recognized in the 2012 Statement of Basis and Purpose that these and other common consent mechanisms could benefit operators (especially smaller ones) and parents if they offer a proper means for providing notice and obtaining verifiable parental consent, as well as ongoing controls for parents to manage their children's accounts. *See* 78 Fed. Reg. 3972, 3989. Remember that, whether or not you use a common consent mechanism to assist in providing notice and obtaining consent, as the operator you are responsible for ensuring that the notice accurately and completely reflects your information collection practices and that the consent mechanism is reasonably designed to reach the parent.

14. Can I apply to the FTC for pre-approval of a new consent mechanism?

Yes. The amended Rule provides a mechanism for interested parties to file a written request for Commission approval of parental consent methods not currently enumerated in 16 C.F.R. § 312.5(b). *See* 16 C.F.R. § 312.12(a).

15. I would like to apply to the FTC for approval of a new method of parental consent that I have developed, but I am concerned about having my trade secrets publicly posted. Is there a way to prevent this?

The Commission recognized this concern in the 2012 Statement of Basis and Purpose, noting that, "just as the Commission has done for COPPA safe harbor applicants, it would permit those entities that voluntarily seek approval of consent mechanisms to seek confidential treatment for those portions of their applications that they believe warrant trade secret protection. In the event an applicant is not comfortable with the Commission's determination as to which materials will be placed on the public record, it will be free to withdraw the proposal from the approval process." *See* 78 Fed. Reg. 3972, 3992.

I. EXCEPTIONS TO PRIOR PARENTAL CONSENT

1. I want to have a contest on my child-directed Web site. Can I use the Rule's "one-time contact" exception to prior parental consent?

Yes, if you properly design your contest. You may use the "one time contact" exception if you collect children's online contact information, and only this information, to enter them in the contest, and then only contact such children once when the contest ends to notify them if they have won or lost. At that point, you must delete the online contact information you have collected.

If, however, you expect to contact the children more than one time, you must use the "multiple-contact" exception, for which you must also collect a parent's online contact information and provide parents with direct notice of your information practices and an opportunity to opt out. In either case, the Rule prohibits you from using the children's online contact information for any other purpose, and requires you to ensure the security of the information, which is particularly important if the contest runs for any length of time.

If you wish to collect any information from children online beyond online contact information in connection with contest entries – such as collecting a winner's home address to mail a prize – you must first provide parents with direct notice and obtain verifiable parental consent, as you would for other types of personal information collection beyond online contact information. If you do need to obtain a mailing address and wish to stay within the one-time exception, you may ask the child to provide his parent's online contact information and use that identifier to notify the parent if the child wins the contest. In your prize notification message to the parent, you may ask the parent to provide a home mailing address to ship the prize, or invite the parent to call a telephone number to provide the mailing information.

2. I have a child-directed Web site that has an "Ask the Author" corner where children can email questions to featured authors. Do I need to provide notice and obtain parental consent?

If you simply answer the child's question and then delete the child's email address (and do not otherwise maintain or store the child's personal information in any form), then you fall into the Rule's "one-time contact" exception and do not need to obtain parental consent.

3. I offer e-cards and the ability for children to forward items of interest to their friends on my child-directed app. Can I take advantage of one of the Rule's exceptions to parental consent or must I notify parents and obtain consent for this activity?

The answer depends on how you design your e-card or forward-to-a-friend system. Any system providing any opportunity to reveal personal information other than the recipient's email address requires you to obtain verifiable consent from the sender's parent (not email plus), and does not fall within one of COPPA's limited exceptions. This means that if your e-card/forward-to-a-friend system permits personal information to be disclosed either in the "from" or "subject" lines, or in the body of the message, then you must notify the sender's parent and obtain verifiable parental consent *before* collecting any personal information from the child.

In order to take advantage of COPPA's "one-time contact exception" for your e-cards, your web form may only collect the recipient's email address (and, if desired, the sender or recipient's first name); you may not collect any other personal information either from the sender or the recipient, including persistent identifiers that track the user over time and across sites. Moreover, in order to meet this one-time contact exception, your e-card system must not allow the sender to enter her full name, her email address, or the recipient's full name. Nor may you allow the sender to freely type messages either in the subject line or in any text fields of the e-card.

Finally, you should send the e-card immediately and automatically delete the recipient's email address immediately after sending. If you choose to retain the recipient's email address until some point in the future (*e.g.*, until the e-card is opened by the recipient, or you allow the sender to indicate a date in the future when the e-card should be sent), then this collection parallels the conditions for the Rule's "multiple contact exception" for obtaining verifiable parental consent. In this scenario, you must collect the sender's parent's email address and provide notice and an opportunity to opt out to the sender's parent *before* the e-card is sent. *See* 1999 Statement of Basis and Purpose, 64 Fed. Reg. 59888, 59902 n.222.

4. I would like to collect email address, but no other personally identifying information, during my Web site's registration process. I intend to use the email address only for the purpose of providing password reminders to users who register on my site. Do I first have to provide notice and obtain parental consent before collecting a child's email address?

If you plan to retain the child's email address in retrievable form after the initial collection, to be used, for example, to email children reminders of their passwords, then you must provide notice to parents and the opportunity to opt out under the Rule's multiple-contact exception. *See* 16 C.F.R. § 312.5(c)(4).

However, you may collect a child's email address to be used to authenticate the child for purposes of generating a password reminder without first providing parental notice and giving a parent the opportunity to opt out if you meet the following conditions: (1) you do not collect any personal information from the child other than the child's email address; (2) the child cannot disclose any personal information on your Web site; and (3) you immediately and permanently alter the email address (*e.g.*, through "hashing") such that it can only be used as a password reminder and cannot be reconstructed into its original form or used to contact the child. You should explain this process in a clear and conspicuous manner, both at the point of collection and in your site's online privacy policy, so that your users and their parents are informed about how the email addresses will be used. This will prevent confusion by visitors and others who may otherwise assume that your site is improperly collecting and retaining email addresses without any form of parental notice.

5. What does "support for the internal operations of the Web site or online service" mean?

"Support for the internal operations of the Web site or online service," as defined in 16 C.F.R. 312.2, means activities necessary for the site or service to maintain or analyze its functioning; perform network communications; authenticate users or personalize content; serve contextual advertising or cap the frequency of advertising; protect the security or integrity of the user, Web site, or online service; ensure legal or regulatory compliance; or fulfill a request of a child as permitted by § 312.5(c)(3) and (4). Persistent identifiers collected for the sole purpose of providing support for the internal operations of the Web site or online service do not require parental consent, so long as no other personal information is collected and the persistent identifiers are not used or disclosed to contact a specific individual, including through behavioral advertising; to amass a profile on a specific individual; or for any other purpose.

6. Can both a child-directed Web site and a third-party plug-in that collect persistent identifiers from users of that child-directed site rely on the Rule's exception for "support for internal operations"?

Yes. A child-directed site and a third-party plug-in collecting persistent identifiers from users of that child-directed site can both rely upon the Rule's "support for internal operations" exception where the only personal information collected from such users are persistent identifiers for purposes outlined in the "support for internal operations" definition. The persistent identifier information collected by the third-party plug-in may in some instances support only the plug-in's internal operations; in other instances, it may support both its own internal operations and the internal operations of the child-directed site.

7. Does the exception for "support for internal operations" allow me to perform, or retain another party to perform, site analytics?

Yes. Where you, a service provider, or a third party collects persistent identifier information from users of your child-directed site to perform analytics encompassed by the Rule's "support for internal operations" definition, and the information is not used for any other purposes not covered by the support for internal operations definition, then you can rely upon the Rule's exemption from parental and consent.

8. I am an ad network that uses persistent identifiers to personalize advertisements on websites. I know that I operate on a child-directed site, but isn't personalization considered "support for internal operations"?

No. The term "support for internal operations" does not include behavioral advertising. The inclusion of personalization within the definition of support for internal operations was intended to permit operators to maintain *user driven* preferences, such as game scores, or character choices in virtual worlds. "Support for internal operations" does, however, include the collection or use of persistent identifiers in connection with serving contextual advertising on the child-directed site.

9. I have a child-directed app and want to send push notifications. Do I need to get parental consent?

The information you collect from the child's device used to send push notifications is online contact information – it permits you to contact the user outside the confines of your app – and is therefore personal information under the Rule. To the extent the child has specifically requested push notifications, however, you may be able to rely on the "multiple-contact" exception to verifiable parental consent, for which you must also collect a parent's online contact information and provide parents with direct notice of your information practices and an opportunity to opt-out. See FAQ H.2. Importantly, in order to fit within this exception, your push notifications must be reasonably related to the content of your app. If you want to combine this online contact information with other personal information collected from the child, you cannot rely on this exception and must provide parents with direct notice and obtain verifiable parental consent prior to sending push notifications to the child.

10. I have a child-directed website. Can I put a plug-in, such as Facebook Like button, on my site without providing notice and obtaining verifiable parental consent?

In determining whether you must provide notice and obtain verifiable parental consent, you will need to evaluate whether any exceptions apply. Section 312.5(c)(8) of the Rule has an exception to its notice and consent requirements where:

1. a third-party operator only collects a persistent identifier and no other personal information;
2. the user affirmatively interacts with that third-party operator to trigger the collection; and
3. the third-party operator has previously conducted an age-screen of the user, indicating the user is not a child.

If the third-party operator meets all of those requirements, and if your site doesn't collect personal information (except for that covered by an exception), you don't need to provide notice or obtain consent.

This exception doesn't apply to types of plug-ins where the third party collects more information than a persistent identifier — for example, where the third party also collects user comments or other user-generated content. In addition, a child-directed website can't rely on this exception to treat particular visitors as adults and track their activities.

If your inclusion of the plug-in satisfies all the criteria of section 312.5(c)(8) outlined above and/or satisfies another exception to the notice and consent requirements in the Rule (see, for example, the "support for internal operations" exception discussed in FAQ I.5 and I.6 above), you do not have to provide notice and obtain verifiable parental consent.

J. PARENTAL ACCESS TO CHILDREN'S PERSONAL INFORMATION

1. Do I have to keep all information I have ever collected online from a child in case a parent may want to see it in the future?

No. As the Commission noted in the 1999 Statement of Basis and Purpose, "if a parent seeks to review his child's personal information after the operator has deleted it, the operator may simply reply that it no longer has any information concerning that child." *See* 64 Fed. Reg. 59888, 59904.

2. What if, despite my most careful efforts, I mistakenly give out a child's personal information to someone who is not that child's parent or guardian?

The Rule requires you to provide parents with a means of reviewing any personal information you collect online from children. Although the Rule provides that the operator must ensure that the requestor is a parent of the child, it also notes that if you follow reasonable procedures in responding to a request for disclosure of this personal information, you will not be liable under any federal or state law if you mistakenly release a child's personal information to a person other than the parent. *See* 16 C.F.R. § 312.6(a)(3)(i) and (b).

K. DISCLOSURE OF INFORMATION TO THIRD PARTIES

1. If I want to share children's personal information with a service provider or a third party, how should I evaluate whether the security measures that entity has in place are "reasonable" under the Rule?

Before sharing information with such entities, you should determine what the service providers' or third parties' data practices are for maintaining the confidentiality and security of the data and preventing unauthorized access to or use of the information. Your expectations for the treatment of the data should be expressly addressed in any contracts that you have with service providers or third parties. In addition, you must use reasonable means, such as periodic monitoring, to confirm that any service providers or third parties with which you share children's personal information maintain the confidentiality and security of that information.

2. I operate an ad network. I discover three months after the effective date of the Rule that I have been collecting personal information via a child-directed website. What are my obligations regarding personal information I collected after the Rule's effective date, but before I discovered that the information was collected via a child-directed site?

Unless an exception applies, you must provide notice and obtain verifiable parental consent if you: (1) continue to collect new personal information via the website, (2) re-collect personal information you collected before, or (3) use or disclose personal information you know to have come from the child-directed site. With respect to (3), you have to obtain verifiable parental consent before using or disclosing previously-collected data only if you have actual knowledge that you collected it from a child-directed site. In contrast, if, for example, you had converted the data about websites visited into interest categories (e.g., sports enthusiast) and no longer have any indication about where the data originally came from, you can continue to use those interest categories without providing notice or obtaining verifiable parental consent. In addition, if you had collected a persistent identifier from a user on the child-directed website, but have not associated that identifier with the website, you can continue to use the identifier without providing notice or obtaining verifiable parental consent.

With respect to the previously-collected personal information you know came from users of a child-directed site, you must comply with parents' requests under 16 C.F.R. § 312.6, including requests to delete any personal information collected from the child, even if you will not be using or disclosing it. Furthermore, as a best practice you should delete personal information you know to have come from the child-directed site.

L. REQUIREMENT TO LIMIT INFORMATION COLLECTION

1. If I operate a social networking service and a parent revokes her consent to my maintaining personal information collected from the child, can I deny that child access to my service?

Yes. If a parent revokes consent and directs you to delete the personal information you had collected from the child, you may terminate the child's use of your service. *See* 16 C.F.R. § 312.6(c).

2. I know that the Rule says I cannot condition a child's participation in a game or prize offering on the child's disclosing more information than is reasonably necessary to participate in those activities. Does this limitation apply to other online activities?

Yes. The applicable Rule provision is not limited to games or prize offerings, but includes "another activity." *See* 16 C.F.R. § 312.7. This means that you must carefully examine the information you intend to collect in connection with every activity you offer in order to ensure that you are only collecting information that is reasonably necessary to participate in that activity. This guidance is in keeping with the Commission's general guidance on data minimization.

M. COPPA AND SCHOOLS

1. Can an operator of a Web site or online service rely upon an educational institution to provide consent to the operator's collection, use or disclosure of personal information from students?

COPPA does not preclude schools from acting as intermediaries between operators and parents in the notice and consent process, or from serving as the parent's agent in the process of collecting personal information online from students in the school context. *See* 1999 Statement of Basis and Purpose, 64 Fed. Reg. 59888, 59903. Determining whether the school may provide consent on behalf of a parent, or whether the operator can rely on the school for consent, will depend on the nature of the relationship between the online service and the school or child, and the nature of the collection, use, or disclosure of the child's personal information. *See* FAQ M.2 below.

Whether the operator is working with the school, or obtaining consent directly from parents, it must provide a complete and accurate disclosure regarding what data is collected from children, how it will be used, and with whom it will be shared. The operator may violate the Rule if it fails to disclose its data collection, use, or disclosure practices to the consenting party.

In addition, the school also must consider its obligations under the Family Educational Rights and Privacy Act (FERPA), which gives parents certain rights with respect to their children's education records. FERPA is administered by the U.S. Department of Education. For general information on FERPA, *see* http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html. Many school systems have implemented Acceptable Use Policies for Internet Use (AUPs) to educate parents and students about in-school Internet use.

2. Under what circumstances can an operator of a Web site or online service rely upon an educational institution to provide consent?

Many school districts contract with third-party Web site operators to offer online programs solely for the benefit of their students and for the school system, for example, homework help lines, individualized education modules, online research and organizational tools, or web-based testing services. Where a school has contracted with an operator to collect personal information from students for the use and benefit of the school, *and for no other commercial purpose*, the operator is not required to obtain consent directly from parents, and can presume that the school's authorization for the collection of students' personal information is based upon the school having obtained the parents' consent. However, the operator must provide the school with full notice of its collection, use, and disclosure practices, so that the school may make an informed decision. The school may also want to inform parents of these practices in its Acceptable Use Policy.

If, however, an operator intends to use or disclose children's personal information for its own commercial purposes in addition to the provision of services to the school, it will need to obtain parental consent.

3. What information should a school seek from an operator before entering into an arrangement that permits the collection, use or disclosure of personal information from students?

A school should be careful to understand how an operator will collect, use, and disclose personal information from its students in deciding whether to use these online technologies with students. Among the questions that a school should ask potential operators are:

- What types of personal information will the operator collect from students?
- How does the operator use this personal information?
- Does the operator use or share the information for commercial purposes not related to the provision of the online services requested by the school? For instance, does it use the students' personal information in connection with online behavioral advertising, or building user profiles for commercial purposes not related to the provision of the online service?
- Does the operator enable parents to review and have deleted the personal information collected from their children?
- What measures does the operator take to protect the security, confidentiality, and integrity of the personal information that it collects?
- What are the operator's data retention and deletion policies for children's personal information?

4. I am an educator and I want students in my school to share information for class projects using a publicly-available online social network that permits children to participate with prior parental consent. Can I register students in lieu of having their parents register them?

This question assumes that your school has not entered into an arrangement with the social network for the provision of school-based activities, but rather that you intend to use a service that is more broadly-available to children and possibly other users. The Commission has recognized the school's ability to act in the stead of parents in order to provide in-school Internet access. However, where the activities and the associated collection or disclosure of children's personal information will extend beyond school-based activities, the school should carefully consider whether it has effectively notified parents of its intent to allow children to participate in such online activities before giving consent on parents' behalf.

N. COPPA SAFE HARBOR PROGRAMS

1. How can I qualify as a Commission-approved COPPA safe harbor program?

To be considered for COPPA safe harbor status, an industry group or other person must submit its self-regulatory guidelines to the FTC for approval. The Rule requires the Commission to publish the safe harbor application in the Federal Register seeking public comment. The Commission then is required to make a written determination on the application within 180 days after its filing.

COPPA safe harbor applications must contain:

- A detailed explanation of the applicant's business model and technological capabilities and mechanisms it will use to assess member operator's information collection practices;
- A copy of the full text of the safe harbor program's guidelines and any accompanying commentary;
- A comparison of each program guideline with each corresponding Rule provision and a statement of how each guideline meets the Rule's requirements; and
- A statement of how the assessment mechanisms and disciplinary consequences provide effective COPPA enforcement.

The amended Rule sets forth the key criteria the FTC will consider in reviewing a safe harbor application:

- Whether the applicant's program includes guidelines that provide substantially the same or greater protection than the standards set forth in the COPPA Rule;
- Whether the program includes an effective, mandatory mechanism to independently assess member operators' compliance with the program's guidelines, which at a minimum must include a comprehensive annual review by the safe harbor program of each member operator;
- Whether the program includes effective disciplinary actions for member operators who do not comply with the safe harbor program guidelines.

See 16 C.F.R. § 312.11.

2. What should I do if I am interested in submitting my self-regulatory program to the FTC for approval under the safe harbor provision?

Information about applying for FTC approval of a safe harbor program is provided in Section 312.11 of the Rule and

online at the COPPA Safe Harbor Program portion of the FTC's Business Center Web site. In addition, you may send an email to CoppaHotLine@ftc.gov , and a member of the FTC staff will help answer your questions.

3. How can I learn about safe harbor programs that have been approved by the Commission?

Information about the applicants who have sought safe harbor status can be found online at the COPPA Safe Harbor Program portion of the FTC's Business Center Web site. The site includes each organization's applications and guidelines, along with comments submitted by the public, and the basis for the Commission's written determination of each application.

Opportunity to Comment

The National Small Business Ombudsman and 10 Regional Fairness Boards collect comments from small businesses about federal compliance and enforcement activities. Each year, the Ombudsman evaluates the conduct of these activities and rates each agency's responsiveness to small businesses. Small businesses can comment to the Ombudsman without fear of reprisal. To comment, call toll-free 1-888-REGFAIR (1-888-734-3247) or go to www.sba.gov/ombudsman.

Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business [PDF]

When it comes to the collection of personal information from children under 13, the Children's Online Privacy Protection Act (COPPA) puts parents in control. The Federal Trade Commission, the nation's consumer protection agency, enforces the COPPA Rule, which spells out what operators of websites and online services must do to protect children's privacy and safety online. For example, if your company is covered by COPPA, you need to have certain information in your privacy policy and get parental consent before collecting some types of information from kids under 13.

Effective July 1, 2013, the FTC updated the COPPA Rule to reflect changes in technology. Violations can result in law enforcement actions, including civil penalties, so compliance counts.

Here's a step-by-step plan for determining if your company is covered by COPPA — and what to do to comply with the Rule.

Table of Contents

Step 1: Determine if Your Company is a Website or Online Service that Collects Personal Information from Kids Under 13.

Step 2: Post a Privacy Policy that Complies with COPPA.

Step 3: Notify Parents Directly Before Collecting Personal Information from Their Kids.

Step 4: Get Parents' Verifiable Consent Before Collecting Information from Their Kids.

Step 5: Honor Parents' Ongoing Rights with Respect to Information Collected from Their Kids.

Step 6: Implement Reasonable Procedures to Protect the Security of Kids' Personal Information.

Chart: Limited Exceptions to COPPA's Verifiable Parental Consent Requirement

Step 1: Determine if Your Company is a Website or Online Service that Collects Personal Information from Kids Under 13.

COPPA doesn't apply to everyone operating a website or other online service. Put simply, COPPA applies to operators of websites and online services that collect personal information from kids under 13. Here's a more specific way of determining if COPPA applies to you. You must comply with COPPA if:

> Your website or online service is directed to children under 13 and you collect personal information from them.
>
> **OR**
>
> Your website or online service is directed to children under 13 and you let others collect personal information from them.
>
> **OR**
>
> Your website or online service is directed to a general audience, but you have actual knowledge that you collect personal information from children under 13.
>
> **OR**
>
> Your company runs an ad network or plug-in, for example, and has actual knowledge that you collect personal information from users of a website or service directed to children under 13.

To determine if you're covered by COPPA, look at how the Rule defines some key terms.

"Website or online service"

COPPA defines this term broadly. In addition to standard websites, examples of others covered by the Rule include:

- mobile apps that send or receive information online (like network-connected games, social networking apps, or apps that deliver behaviorally-targeted ads),
- internet-enabled gaming platforms,
- plug-ins,
- advertising networks,
- internet-enabled location-based services,
- voice-over internet protocol services.

"Directed to children under 13"

The FTC looks at a variety of factors to see if a site or service is directed to children under 13, including the subject matter of the site or service, visual and audio content, the use of animated characters or other child-oriented activities and incentives, the age of models, the presence of child celebrities or celebrities who appeal to kids, ads on the site or service that are directed to children, and other reliable evidence about the age of the actual or intended audience.

"Personal information"

Each of these is considered personal information under COPPA:

- full name;
- home or other physical address, including street name and city or town,
- online contact information like an email address or other identifier that permits someone to contact a person directly — for example, an IM identifier, VoIP identifier, or video chat identifier;
- screen name or user name where it functions as online contact information;
- telephone number;
- Social Security number;
- a persistent identifier that can be used to recognize a user over time and across different sites, including a cookie number, an IP address, a processor or device serial number, or a unique device identifier;
- a photo, video, or audio file containing a child's image or voice;
- geolocation information sufficient to identify a street name and city or town; or
- other information about the child or parent that is collected from the child and is combined with one of these identifiers.

"Collect"

Under COPPA, you're collecting information if you:

- request, prompt, or encourage the submission of information, even if it's optional;
- let information be made publicly available (for example, with an open chat or posting function) unless you take reasonable measures to delete all or virtually all personal information before postings are public and delete all information from your records; or
- passively track a child online.

If another company collects personal information through your child-directed site or service — through an ad network or plug-in, for example — you're responsible for complying with COPPA. If you have actual knowledge that you're collecting personal information directly from users of a child-directed site or service, you're responsible for complying with COPPA, too.

Step 2: Post a Privacy Policy that Complies with COPPA.

Assuming you're covered by COPPA, the next step is to post a privacy policy. It must clearly and comprehensively describe how personal information collected online from kids under 13 is handled. The notice must describe not only *your* practices, but also the practices of any others collecting personal information on your site or service — for example, plug-ins or ad networks.

Include a link to your privacy policy on your homepage and anywhere you collect personal information from children. If you operate a site or service directed to a general audience, but have a separate section for kids, post a link to your privacy policy on the homepage of the kids' part of your site or service.

Make those links clear and prominent. Consider using a larger font or a different color type on a contrasting background. A fineprint link at the bottom of the page or a link that isn't distinguishable from other links on your site won't do the trick.

To comply with COPPA, your privacy policy should be clear and easy to read. Don't add any unrelated or confusing information. Here's what your policy must include:

- **A list of all operators collecting personal information.** Name each operator collecting or maintaining

children's personal information through your site or service. For each operator, include a name and contact information (address, telephone number, and email address). If more than one operator is collecting information, it's okay to give contact information for only one as long as that operator will respond to all inquiries from parents about your site or service's practices. Even so, you still have to list all the operators in your privacy policy.

- **A description of the personal information collected and how it's used.** Your policy must describe:
  - the types of personal information collected from children (for example, name, address, email address, hobbies, etc.);
  - how the personal information is collected — directly from the child or passively, say, through cookies;
  - how the personal information will be used (for example, for marketing to the child, notifying contest winners, or allowing the child to make information publicly available through a chat room); and
  - whether you disclose personal information collected from kids to third parties. If you do, your privacy policy must list the types of businesses you disclose information to (for example, ad networks) and how they use the information.
- **A description of parental rights.** Your privacy policy must tell parents:
  - that you won't require a child to disclose more information than is reasonably necessary to participate in an activity;
  - that they can review their child's personal information, direct you to delete it, and refuse to allow any further collection or use of the child's information;
  - that they can agree to the collection and use of their child's information, but still not allow disclosure to third parties unless that's part of the service (for example, social networking); and
  - the procedures to follow to exercise their rights.

Step 3: Notify Parents Directly Before Collecting Personal Information from Their Kids.

COPPA requires that you give parents "direct notice" before collecting information from their kids. In addition, if you make a material change to the practices parents previously agreed to, you have to send an updated direct notice.

The notice should be clear and easy to read. Don't include any unrelated or confusing information. The notice must tell parents:

- that you collected their online contact information for the purpose of getting their consent;
- that you want to collect personal information from their child;
- that their consent is required for the collection, use, and disclosure of the information;
- the specific personal information you want to collect and how it might be disclosed to others;
- a link to your online privacy policy;
- how the parent can give their consent; and
- that if the parent doesn't consent within a reasonable time, you'll delete the parent's online contact information from your records.

In certain circumstances, it's okay under COPPA to collect a narrow class of personal information without getting parental consent. But you may still have to give parents direct notice of your activities. (See the chart at the end for a list of those limited exceptions.)

Step 4: Get Parents' Verifiable Consent Before Collecting Information from Their Kids.

Before collecting, using or disclosing personal information from a child, you must get their parent's verifiable consent. How do you get that? COPPA leaves it up to you, but it's important to choose a method reasonably designed in light of available technology to ensure that the person giving the consent is the child's parent. If you have actual knowledge that you're collecting personal information from a site or service that is directed to children, you may get consent directly or through the child-directed site or service.

Acceptable methods include having the parent:

- sign a consent form and send it back to you via fax, mail, or electronic scan;
- use a credit card, debit card, or other online payment system that provides notification of each separate transaction to the account holder;
- call a toll-free number staffed by trained personnel;
- connect to trained personnel via a video conference; or
- provide a copy of a form of government issued ID that you check against a database, as long as you delete the identification from your records when you finish the verification process.

If you will use a child's personal information only for internal purposes and won't disclose it, you may use a method known as "email plus." Under that method, send an email to the parent and have them respond with their consent. Then you must send a confirmation to the parent via email, letter, or phone call. If you use email plus, you must let the parent

know they can revoke their consent anytime.

You must give parents the option of allowing the collection and use of their child's personal information without agreeing to disclosing that information to third parties. If you make changes to the collection, use, or disclosure practices the parent already agreed to, you must send the parent a new notice and get their consent.

Check the chart for the narrow exceptions to the general rule that you must get parental consent before collecting personal information from kids. Even if you fall within an exception to the consent requirement, you still may have specific notice requirements.

Step 5: Honor Parents' Ongoing Rights with Respect to Information Collected from Their Kids.

Even if parents have agreed that you may collect information from their kids, parents have ongoing rights — and you have continuing obligations.

If a parent asks, you must:

- give them a way to review the personal information collected from their child;
- give them a way to revoke their consent and refuse the further use or collection of personal information from their child; and
- delete their child's personal information.

Any time you're communicating with a parent about personal information already collected from their child, take reasonable steps to ensure you're dealing with the child's parent. At the same time, make sure the method you use to give parents access to information collected from their kids isn't unduly burdensome on the parent. Under COPPA, it may be okay to terminate a service to a child if the parent revokes consent, but only if the information at issue is reasonably necessary for the child's participation in that activity.

Step 6: Implement Reasonable Procedures to Protect the Security of Kids' Personal Information.

COPPA requires you to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children. Minimize what you collect in the first place. Take reasonable steps to release personal information only to service providers and third parties capable of maintaining its confidentiality, security, and integrity. Get assurances they'll live up to those responsibilities. Hold on to personal information only as long as is reasonably necessary for the purpose for which it was collected. Securely dispose of it once you no longer have a legitimate reason for retaining it.

Looking for more about the Children's Online Privacy Protection Rule? Visit the Children's Privacy page of the FTC's Business Center. For additional advice, read Complying with COPPA: Frequently Asked Questions. Visit OnGuard Online.gov for general information about protecting kids' privacy online. Email us at COPPAhotline@ftc.gov if you have other questions.

Chart: Limited Exceptions to COPPA's Verifiable Parental Consent Requirement

In general, you must get a parent's verifiable consent before collecting personal information from their child. But there are some limited exceptions to that requirement that allow you to collect information without parental consent. Keep in mind that the kind of information you may collect under each exception is narrow. You can't collect anything more. Also, if you collect information under one of these exceptions, you can't use it or disclose it for any other purpose.

Reason you may collect information without parental consent	**The kind of information you may collect**	**Limits on how you may use the information**	**If you collect information under this exception, what you must tell parents in your direct notice**
To get verifiable parental consent	child's and parent's name and online contact information	You must delete their contact information if you don't get consent within a reasonable time.	
To give voluntary notice to a parent about their child's participation on a site or service that doesn't collect personal information	parent's online contact information	You can't otherwise collect, use, or disclose the information.	You must: • tell parents you collected their online contact information to let them know about their child's activities on a site or service that doesn't collect personal information;

			• tell them their online contact information won't be used for any other purpose; • tell them they may refuse their child's participation and require that you delete their contact information; and • hyperlink to your privacy policy.
To respond directly to a child's specific one-time request (for example, if the child wants to enter a contest)	child's online contact information	You can't use the information to contact the child again and you must delete it after you respond to the request.	
To respond directly more than once to a child's specific request (for example, if the child want to receive a newsletter)	child's and parent's online contact information		You must: • tell parents you collected their online contact information to let them know their child has asked for multiple online communications; • tell parents you collected their child's online contact information to provide the multiple communications they asked for; • tell parents the online contact information won't be used for any other purpose and won't be disclosed or combined with other information; • tell parents that if they don't opt out, you may use the child's online contact information for that purpose; and • hyperlink to your privacy policy.
To protect a child's safety	child's and parent's name and online contact information		You must: • tell parents you collected the names and contact information to protect a child's safety; • tell parents the information won't be used or disclosed for any other purpose; • tell parents they may refuse to permit the use of the contact information and require you to delete it; and • hyperlink to your

			privacy policy
To protect the security or integrity of your site or service, to take precautions against liability, to respond to judicial process, or — as permitted by law — to provide information to law enforcement	child's name and online contact information	You can't use the information to contact a specific person, conduct behavioral advertising, or amass a profile on a person. You can't use personal information other than a persistent identifier for this exception.	
To provide support for internal operations of your site or service. **This includes:** • **maintaining or analyzing the functioning of the site,** • **performing network communications,** • **authenticating users of the site or personalizing content,** • **serving contextual ads or frequency capping,** • **protecting the security or integrity of the user or the site** • **legal or regulatory compliance, or** • **fulfilling a child's request under the one-time contact or multiple contact exceptions.**	persistent identifier		
If you have actual knowledge that a person's information was collected through a child-directed site, but their previous registration indicates the person is 13 or over **This exception applies only if:** • **you collect only a persistent identifier and no other personal information;** • **the person affirmatively interacts with your site or service to trigger the collection; and** • **you have already conducted an age-screen of the person indicating he or she is 13 or over.**	persistent identifier	You can't collect other personal information.	

For More Information

The FTC works for the consumer to prevent fraudulent, deceptive, and unfair practices in the marketplace and to provide information to businesses to help them comply with the law. To file a complaint, visit ftc.gov or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. Watch a video, How to File a Complaint, to learn more. The FTC enters consumer complaints into the Consumer Sentinel Network, a secure online database and investigative tool used by hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

Your Opportunity to Comment

The National Small Business Ombudsman and 10 Regional Fairness Boards collect comments from small businesses about federal compliance and enforcement activities. Each year, the Ombudsman evaluates the conduct of these activities and rates each agency's responsiveness to small businesses. Small businesses can comment to the Ombudsman without fear of reprisal. To comment, call toll-free 1-888-REGFAIR (1-888-734-3247) or go to www.sba.gov/ombudsman.

June 2013

Fighting Identity Theft with the Red Flags Rule: A How-To Guide for Business

An estimated nine million Americans have their identities stolen each year. Identity thieves may drain accounts, damage credit, and even put medical treatment at risk. The cost to business — left with unpaid bills racked up by scam artists — can be staggering, too.

The Red Flags Rule[1] requires many businesses and organizations to implement a written identity theft prevention program designed to detect the "red flags" of identity theft in their day-to-day operations, take steps to prevent the crime, and mitigate its damage. The bottom line is that a program can help businesses spot suspicious patterns and prevent the costly consequences of identity theft.

The Federal Trade Commission (FTC) enforces the Red Flags Rule with several other agencies. This article has tips for organizations under FTC jurisdiction to determine whether they need to design an identity theft prevention program.

Table of Contents

An Overview

Who Must Comply with the Red Flags Rule

FAQs

How To Comply: A Four-Step Process

Endnotes

An Overview

The Red Flags Rule tells you how to develop, implement, and administer an identity theft prevention program. A program must include four basic elements that create a framework to deal with the threat of identity theft.[2]

1. A program must include reasonable policies and procedures to identify the red flags of identity theft that may occur in your day-to-day operations. Red Flags are suspicious patterns or practices, or specific activities that indicate the possibility of identity theft.[3] For example, if a customer has to provide some form of identification to open an account with your company, an ID that doesn't look genuine is a "red flag" for your business.
2. A program must be designed to detect the red flags you've identified. If you have identified fake IDs as a red flag, for example, you must have procedures to detect possible fake, forged, or altered identification.
3. A program must spell out appropriate actions you'll take take when you detect red flags.
4. A program must detail how you'll keep it current to reflect new threats.

Just getting something down on paper won't reduce the risk of identity theft. That's why the Red Flags Rule has requirements on how to incorporate your program into the daily operations of your business. Fortunately, the Rule also gives you the flexibility to design a program appropriate for your company — its size and potential risks of identity theft. While some businesses and organizations may need a comprehensive program to address a high risk of identity theft, a streamlined program may be appropriate for businesses facing a low risk.

Securing the data you collect and maintain about customers is important in reducing identity theft. The Red Flags Rule seeks to prevent identity theft, too, by ensuring that your business or organization is on the lookout for the signs that a crook is using someone else's information, typically to get products or services from you without paying for them. That's why it's important to use a one-two punch in the battle against identity theft: implement data security practices that make it harder for crooks to get access to the personal information they use to open or access accounts, and pay attention to the red flags that suggest that fraud may be afoot.

Who Must Comply with the Red Flags Rule: A Two-Part Analysis

The Red Flags Rule requires "financial institutions" and some "creditors" to conduct a periodic risk assessment to determine if they have "covered accounts." The determination isn't based on the industry or sector, but rather on whether a business' activities fall within the relevant definitions. A business must implement a written program **only** if it has covered accounts.

Financial Institution

The Red Flags Rule defines a "financial institution" as a state or national bank, a state or federal savings and loan association, a mutual savings bank, a state or federal credit union, or a person that, directly or indirectly, holds a transaction account belonging to a consumer.[4] While many financial institutions are under the jurisdiction of the federal bank regulatory agencies or other federal agencies, state-chartered credit unions are one category of financial institution under the FTC's jurisdiction.

Creditor

The Red Flags Rule defines "creditor" based on conduct.[5]

To determine if your business is a creditor under the Red Flags Rule, ask these questions:

Does my business or organization regularly:

- defer payment for goods and services or bill customers?
- grant or arrange credit?
- participate in the decision to extend, renew, or set the terms of credit?

If you answer:

- No to all, the Rule does not apply.
- Yes to one or more, ask:

Does my business or organization regularly and in the ordinary course of business:

- get or use consumer reports in connection with a credit transaction?
- give information to credit reporting companies in connection with a credit transaction?
- advance funds to — or for — someone who must repay them, either with funds or pledged property (excluding incidental expenses in connection with the services you provide to them)?

If you answer:

- No to all, the Rule does not apply.
- Yes to one or more, you are a creditor covered by the Rule.

Covered Accounts

If you conclude that your business or organization is a financial institution or a creditor covered by the Rule, you must determine if you have any "covered accounts," as the Red Flags Rule defines that term. You'll need to look at existing accounts **and** new ones[6]. Two categories of accounts are covered:

1. A consumer account for your customers for personal, family, or household purposes that involves or allows multiple payments or transactions.[7] Examples are credit card accounts, mortgage loans, automobile loans, checking accounts, and savings accounts.
2. "Any other account that a financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks."[8] Examples include small business accounts, sole proprietorship accounts, or single transaction consumer accounts that may be vulnerable to identity theft. Unlike consumer accounts designed to allow multiple payments or transactions — always considered "covered accounts" under the Rule — other types of accounts are "covered" only if the risk of identity theft is reasonably foreseeable.

In determining if accounts are covered under the second category, consider how they're opened and accessed. For example, there may be a reasonably foreseeable risk of identity theft in connection with business accounts that can be accessed remotely — say, through the Internet or the telephone. Your risk analysis must consider any actual incidents of identity theft involving accounts like these.

If you don't have any covered accounts, you don't need a written program. But business models and services change. You may acquire covered accounts through changes to your business structure, process, or organization. That's why it's good policy and practice to conduct a periodic risk assessment.

FAQs

1. **I review credit reports to screen job applicants. Does the Rule apply to my business on this basis alone?**

   No, the Rule does not apply because the use is not "in connection with a credit transaction."

2. **What if I *occasionally* get credit reports in connection with credit transactions?**

   According to the Rule, these activities must be done "regularly and in the ordinary course of business." Isolated conduct does not trigger application of the Rule, but if your business regularly furnishes delinquent account information to a consumer reporting company but no other credit information, that satisfies the "regularly and in the ordinary course of business" prerequisite.

   What is deemed "regularly and in the ordinary course of business" is specific to individual companies. If you get consumer reports or furnish information to a consumer reporting company regularly and in the ordinary course of your particular business, the Rule applies, even if for others in your industry it isn't a regular practice or part of the ordinary course of business.

3. **I am a professional who bills my clients for services at the end of the month. Am I a creditor just because I allow clients to pay later?**

   No. Deferring payment for goods or services, payment of debt, or the purchase of property or services alone doesn't constitute "advancing funds" under the Rule.

4. **In my business, I lend money to customers for their purchases. The loans are backed by title to their car. Is this considered "advancing funds"?**

   Yes. Anyone who lends money — like a payday lender or automobile title lender — is covered by the Rule. Their lending activities may make their business attractive targets for identity theft. But deferring the payment of debt or the purchase of property or services alone doesn't constitute "advancing funds."

5. **I offer instant credit to my customers and contract with another company to pull credit reports to determine their creditworthiness. No one in our organization ever sees the credit reports. Is my business covered by the Rule**?

   Yes. Your business is — regularly and in the ordinary course of business — using credit reports in connection with a credit transaction. The Rule applies whether your business uses the reports directly or whether a third-party evaluates them for you.

6. **I operate a finance company that helps people buy furniture. Does the Rule apply to my business?**

   Yes. Your company's financing agreements are considered to be "advancing funds on behalf of a person."

7. **In my legal practice, I often make copies and pay filing, court, or expert fees for my clients. Am I "advancing funds"?**

   No. This is not the same as a commercial lender making a loan; "advancing funds" does not include paying in advance for fees, materials, or services that are incidental to providing another service that someone requested.

8. **Our company is a "creditor" under the Rule and we have credit and non-credit accounts. Do we have to determine if both types of accounts are "covered accounts"?**

   Yes. You must examine all your accounts to determine which are "covered accounts" that must be included in your written identity theft prevention program.

9. **My business accepts credit cards for payments. Are we covered by the Red Flags Rule on this basis alone?**

   No. Just accepting credit cards as a form of payment does not make you a "creditor" under the Red Flags Rule.

10. **My business isn't subject to much of a risk that a crook is going to misuse someone's identity to steal from me, but it does have covered accounts. How should I structure my program?**

    If identity theft isn't a big risk in your business, complying with the Rule is simple and straightforward. For example, if the risk of identity theft is low, your program might focus on how to respond if you are notified — say, by a customer or a law enforcement officer — that someone's identity was misused at your business. The Guidelines to the Rule have examples of possible responses. But even a business at low risk needs a written program that is approved either by its board of directors or an appropriate senior employee.

How To Comply: A Four-Step Process

Many companies already have plans and policies to combat identity theft and related fraud. If that's the case for your business, you're already on your way to full compliance.

1. Identify Relevant Red Flags

What are "red flags"? They're the potential patterns, practices, or specific activities indicating the possibility of identity theft.[9] Consider:

Risk Factors. Different types of accounts pose different kinds of risk. For example, red flags for deposit accounts may differ from red flags for credit accounts, and those for consumer accounts may differ from those for business accounts. When you are identifying key red flags, think about the types of accounts you offer or maintain; the ways you open covered accounts; how you provide access to those accounts; and what you know about identity theft in your business.

Sources of Red Flags. Consider other sources of information, including the experience of other members of your industry. Technology and criminal techniques change constantly, so it's important to keep up-to-date on new threats.

Categories of Common Red Flags. Supplement A to the Red Flags Rule lists specific categories of warning signs to consider including in your program. The examples here are one way to think about relevant red flags in the context of your own business.

- **Alerts, Notifications, and Warnings from a Credit Reporting Company**. Changes in a credit report or a consumer's credit activity might signal identity theft:
    - a fraud or active duty alert on a credit report
    - a notice of credit freeze in response to a request for a credit report
    - a notice of address discrepancy provided by a credit reporting company
    - a credit report indicating a pattern inconsistent with the person's history B for example, an increase in the volume of inquiries or the use of credit, especially on new accounts; an unusual number of recently established credit relationships; or an account that was closed because of an abuse of account privileges
- **Suspicious Documents**. Documents can offer hints of identity theft:
    - identification looks altered or forged
    - the person presenting the identification doesn't look like the photo or match the physical description
    - information on the identification differs from what the person with identification is telling you or doesn't match a signature card or recent check
    - an application looks like it's been altered, forged, or torn up and reassembled
- **Personal Identifying Information**. Personal identifying information can indicate identity theft:
    - inconsistencies with what you know — for example, an address that doesn't match the credit report or the use of a Social Security number that's listed on the Social Security Administration Death Master File
    - inconsistencies in the information a customer has submitted to you
    - an address, phone number, or other personal information already used on an account you know to be fraudulent
    - a bogus address, an address for a mail drop or prison, a phone number that's invalid, or one that's associated with a pager or answering service
    - a Social Security number used by someone else opening an account
    - an address or telephone number used by several people opening accounts
    - a person who omits required information on an application and doesn't respond to notices that the application is incomplete
    - a person who can't provide authenticating information beyond what's generally available from a wallet or credit report — for example, someone who can't answer a challenge question
- **Account Activity**. How the account is being used can be a tip-off to identity theft:
    - shortly after you're notified of a change of address, you're asked for new or additional credit cards, or to add users to the account
    - a new account used in ways associated with fraud — for example, the customer doesn't make the first payment, or makes only an initial payment; or most of the available credit is used for cash advances or for jewelry, electronics, or other merchandise easily convertible to cash
    - an account used outside of established patterns — for example, nonpayment when there's no history of missed payments, a big increase in the use of available credit, or a major change in buying or spending patterns or electronic fund transfers
    - an account that is inactive is used again
    - mail sent to the customer that is returned repeatedly as undeliverable although transactions continue to be conducted on the account
    - information that the customer isn't receiving an account statement by mail or email
    - information about unauthorized charges on the account
- **Notice from Other Sources.** A customer, a victim of identity theft, a law enforcement authority, or someone else may be trying to tell you that an account has been opened or used fraudulently.

2. Detect Red Flags

Sometimes, using identity verification and authentication methods can help you detect red flags. Consider whether your procedures should differ if an identity verification or authentication is taking place in person, by telephone, mail, or online.

- **New accounts.** When verifying the identity of the person who is opening a new account, reasonable procedures may include getting a name, address, and identification number and, for in-person verification, checking a current government-issued identification card, like a driver's license or passport. Depending on the circumstances, you may want to compare that to information you can find out from other sources, like a credit reporting company or data broker, or the Social Security Number Death Master File.[10] Asking questions based on information from other sources can be a helpful way to verify someone's identity.
- **Existing accounts.** To detect red flags for existing accounts, your program may include reasonable procedures to confirm the identity of the person you're dealing with, to monitor transactions, and to verify the validity of change-of-address requests. For online authentication, consider the Federal Financial Institutions Examination Council's guidance on authentication as a starting point.[11] It explores the application of multi-factor authentication techniques in high-risk environments, including using passwords, PINs, smart cards, tokens, and biometric identification. Certain types of personal information — like a Social Security number, date of birth, mother's maiden name, or mailing address — are not reliable authenticators because they're so easily accessible.

You may be using programs to monitor transactions, identify behavior that indicates the possibility of fraud and identity theft, or validate changes of address. If so, incorporate these tools into your program.

3. Prevent And Mitigate Identity Theft

When you spot a red flag, be prepared to respond appropriately. Your response will depend on the degree of risk posed. It may need to accommodate other legal obligations, like laws about providing and terminating service.

The Guidelines in the Red Flags Rule offer examples of some appropriate responses, including:

- monitoring a covered account for evidence of identity theft
- contacting the customer
- changing passwords, security codes, or other ways to access a covered account
- closing an existing account
- reopening an account with a new account number
- not opening a new account
- not trying to collect on an account or not selling an account to a debt collector
- notifying law enforcement
- determining that no response is warranted under the particular circumstances

The facts of a particular case may warrant using one of these options, several of them, or another response altogether. Consider whether any aggravating factors raise the risk of identity theft. For example, a recent breach that resulted in unauthorized access to a customer's account records would call for a stepped-up response because the risk of identity theft rises, too.

4. Update The Program

The Rule recognizes that new red flags emerge as technology changes or identity thieves change their tactics, and requires periodic updates to your program. Factor in your own experience with identity theft; changes in how identity thieves operate; new methods to detect, prevent, and mitigate identity theft; changes in the accounts you offer; and changes in your business, like mergers, acquisitions, alliances, joint ventures, and arrangements with service providers.

Administering Your Program

Your Board of Directors — or an appropriate committee of the Board — must approve your initial plan. If you don't have a board, someone in senior management must approve it. The Board may oversee, develop, implement, and administer the program — or it may designate a senior employee to do the job. Responsibilities include assigning specific responsibility for the program's implementation, reviewing staff reports about compliance with the Rule, and approving important changes to your program.

The Rule requires that you train relevant staff only as "necessary." Staff who have taken fraud prevention training may not need to be re-trained. Remember that employees at many levels of your organization can play a key role in identity theft deterrence and detection.

In administering your program, monitor the activities of your service providers. If they're conducting activities covered by the Rule — for example, opening or managing accounts, billing customers, providing customer service, or collecting debts — they must apply the same standards you would if you were performing the tasks yourself. One way to make sure your service providers are taking reasonable steps is to add a provision to your contracts that they have procedures in place to detect red flags and either report them to you or respond appropriately to prevent or mitigate the crime. Other ways to monitor your service providers include giving them a copy of your program, reviewing the red flag policies, or requiring periodic reports about red flags they have detected and their response.

It's likely that service providers offer the same services to a number of client companies. As a result, the Guidelines are flexible about service providers using their own programs as long as they meet the requirements of the Rule.

The person responsible for your program should report at least annually to your Board of Directors or a designated senior manager. The report should evaluate how effective your program has been in addressing the risk of identity theft; how you're monitoring the practices of your service providers; significant incidents of identity theft and your response; and recommendations for major changes to the program.[12]

FTC Resources

Identity Theft
ftc.gov/idtheft

Endnotes

1 The Red Flags Rule was issued in 2007 under Section 114 of the Fair and Accurate Credit Transaction Act of 2003 (FACT Act), Pub. L. 108-159, amending the Fair Credit Reporting Act (FCRA), 15 U.S.C. ' 1681m(e). The Red Flags Rule is published at 16 C.F.R. ' 681.1. See also 72 Fed. Reg. at 63,771 (Nov. 9, 2007). You can find the full text at http://www.ftc.gov/os/fedreg/2007/november/071109redflags.pdf. The preamble B pages 63,718-63,733 — discusses the purpose, intent, and scope of coverage of the Rule. The text of the FTC rule is at pages 63,771-63,774. The Rule includes Guidelines B Appendix A, pages 63,773-63,774 — intended to help businesses develop and maintain a compliance program. The Supplement to the Guidelines — page 63,774 — provides a list of examples of red flags for businesses and organizations to consider incorporating into their program. This guide does not address companies' obligations under the Address Discrepancy or the Card Issuer Rule, also contained in the Federal Register with the Red Flags Rule.

The Rule was amended in 2010 by the Red Flag Program Clarification Act of 2010, 15 U.S.C. 1681m(e)(4), Pub. L. 111-319, 124 Stat. 3457 (Dec. 18, 2010).

2 "Identity theft" means a fraud committed or attempted using the identifying information of another person without authority. See 16 C.F.R. ' 603.2(a). "Identifying information" means "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including any —

(1) Name, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;

(2) Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;

(3) Unique electronic identification number, address, or routing code; or

(4) Telecommunication identifying information or access device (as defined in 18 U.S.C. 1029(e))."

See 16 C.F.R. ' 603.2(b).

3 See 16 C.F.R. ' 681.1(b)(9).

4 The Rule definition of "financial institution" is found in the FCRA. See 15 U.S.C. ' 1681a(t). The term "transaction" is defined in section 19(b) of the Federal Reserve Act. See 12 U.S.C. ' 461(b)(1)(C). A "transaction account" is a deposit or account from which owners may make payments or transfers to third parties or others. Transaction accounts include checking accounts, negotiable orders of withdrawal accounts, savings deposits subject to automatic transfers, and share draft accounts.

5 "Creditor" and "credit" are defined in the FCRA, see 15 U.S.C. 1681a(r)(5), by reference to section 702 of the Equal Credit Opportunity Act (ECOA), 15 U.S.C. ' 1691a. The ECOA defines "credit" as "the right granted by a creditor to a debtor to defer payment of debt or to incur debts and defer its payment or to purchase property or services and defer payment therefor." 15 U.S.C. ' 1691a(d). The ECOA defines "creditor" as "any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of any original creditor who participates in the decision to extend, renew, or continue credit." 15 U.S.C. ' 1691a(e). The term "person" means "a natural person, a corporation, government or governmental subdivision or agency, trust, estate, partnership, cooperative, or association." 15 U.S.C. ' 1691a(f). See also Regulation B. 68 Fed. Reg. 13,161 (Mar. 18, 2003).

The Clarification Act has modified the definition of "creditor" however. For purposes of the Red Flags Rule, a creditor —

> "A. means a creditor, as defined in section 702 of the [ECOA], that regularly and in the ordinary course of business—
>
> > (i) obtains or uses consumer reports, directly or indirectly, in connection with a credit transaction;
> >
> > (ii) furnishes information to consumer reporting agencies, as described in section 623 [of the FCRA], in connection with a credit transaction; or
> >
> > (iii) advances funds to or on behalf of a person, based on an obligation of the person to repay the funds or repayable from specific property pledged by or on behalf of the person;
>
> B. does not include a creditor ... that advances funds on behalf of a person for expenses incidental to a service provided by the creditor to that person."

6 An "account" is a continuing relationship established by a person with a financial institution or creditor to obtain a product or service for personal, family, household, or business purposes. 16 C.F.R. ' 681.1(b)(1). An account does not include a one-time transaction involving someone who isn't your customer, such as a withdrawal from an ATM machine.

7 See 16 C.F.R. ' 681.1(b)(3)(i).

8 16 C.F.R. ' 681.1(b)(3)(ii).

9 See 16 C.F.R. ' 681.12(b)(9).

10 The verification procedures are set forth in the Customer Identification Programs Rule applicable to banking institutions, 31 C.F.R. ' 103.121. This Rule may be a helpful starting point in developing your program.

11 “Authentication in an Internet Banking Environment” (Oct. 2, 2005) available at http://www.ffiec.gov/pdf/authentication_guidance.pdf.

12 See 72 Fed. Reg. at 63,773.

May 2013

EnergyGuide Labeling: FAQs for Appliance Manufacturers

The Energy Labeling Rule requires manufacturers of certain appliances to disclose a product's annual energy cost or efficiency information — based on Department of Energy (DOE) test procedures — on EnergyGuide labels, and to report their findings to the FTC.

Those bright yellow EnergyGuide labels show consumers how much it might cost to run an appliance each year based on how much energy it uses, and they make it easier for shoppers to compare the energy use among similar models.

To help you better understand your responsibilities under the Rule, Federal Trade Commission (FTC) staff have prepared answers to some questions we've been asked. For questions about DOE test procedures and conservation standards, DOE is the best source of information: EERE_ACES@ee.doe.gov .

Table of Contents

Which products must have EnergyGuide labels?

Where can I get a copy of the EnergyGuide label?

How do I label my product if its annual energy cost or efficiency falls outside of the given range in the Energy Labeling Rule?

Do I need to get my labels approved by the FTC before I put them on my products?

Am I required to post copies of the EnergyGuide label for my products online? If so, for how long?

What information do websites and catalogs that sell products with EnergyGuide labels need to include?

When must I report annual energy cost or efficiency information to the FTC?

How do I report appliance data to the FTC?

Which products must have EnergyGuide labels?

The Rule requires EnergyGuide labels for clothes washers, refrigerators, freezers, televisions, water heaters, dishwashers, room air conditioners, central air conditioners, furnaces, boilers, heat pumps, and pool heaters. Labeling requirements for certain light bulbs are explained here. The Rule also covers labeling for plumbing products and ceiling fans. See 16 CFR Part 305

Where can I get a copy of the EnergyGuide label?

The FTC offers templates to download and create your EnergyGuide labels. You also can look at samples of the EnergyGuide label in Appendix L of the Rule. You are responsible for producing your own labels for your products in accordance with the specific requirements in the Energy Labeling Rule.

How do I label my product if its annual energy cost or efficiency falls outside of the given range in the Energy Labeling Rule?

When the estimated annual operating cost or energy efficiency rating of a product is outside the current range for that product on the EnergyGuide label (which might result from the introduction of a new or changed model), you must:

- not place the product on the label's scale, and
- add the appropriate sentence in the space just below the scale on the label:

  The estimated yearly operating cost of this model was not available when the range was published.

  OR

The energy efficiency rating of this model was not available when the range was published.

See Appendix L of the Energy Labeling Rule for a sample label.

Do I need to get my labels approved by the FTC before I put them on my products?

No. The Energy Labeling Rule doesn't require FTC approval. However, manufacturers must follow DOE's testing and certification requirements and the FTC's requirements for reporting energy consumption information before distributing appliances.

Am I required to post copies of the EnergyGuide label for my products online? If so, for how long?

By July 13, 2013, you must post images of the EnergyGuide labels for products on a publicly available website in a way that allows retailers to hyperlink to the label or download it. The label for a specific model must remain on the website for six months after production ends. See 16 CFR § 305.6

What information do websites and catalogs that sell products with EnergyGuide labels need to include?

Any manufacturer, distributor, retailer, or private labeler who advertises a product with an EnergyGuide label on a website or in a print catalog must disclose clearly and conspicuously — on the page listing the product — all of the information on the product's EnergyGuide label, or show an image of the EnergyGuide label itself. However, this requirement applies only to websites and print catalogs that contain the terms of sale, retail price, and ordering instructions for consumers.

Starting January 15, 2014, these websites and catalogs must show the EnergyGuide label. The labels must be clear and conspicuous and in close proximity to the product's price on each page that contains a detailed description of the product. If the website hyperlinks to the image of the label, it must use the sample EnergyGuide icon (i.e., web button) provided by the FTC. The website must hyperlink the image so that consumers don't have to save the hyperlinked image to view it. See 16 CFR § 305.20

When must I report annual energy cost or efficiency information to the FTC?

The Rule has two reporting requirements:

1. Annual Reports for All Models

You must submit a report each year with information for all appliance models in production. The report also should contain data for models that have been discontinued within the last year.

Due Dates for Annual Reports

Product	Due Date
Ceiling Fans	March 1
Showerheads, Faucets, Water Closets, Urinals	March 1
Water Heaters (all types)	May 1
Pool Heaters	May 1
Furnaces and Boilers	May 1
Dishwashers	June 1
Central Air Conditioners	July 1
Room Air Conditioners	July 1
Heat Pumps	July 1
Refrigerators	August 1
Refrigerator-Freezers	August 1
Freezers	August 1
Clothes Washers	October 1

2. New Model Reports

Before you distribute a new model — or a model subject to design or retrofit alterations that change the energy data —

you must report the energy cost or efficiency of the model to the FTC. Reported data is public information. See 16 CFR § 305.8

How do I report appliance data to the FTC?

You can submit reports required by the FTC through the Department of Energy's Compliance Certification Management System (CCMS) at https://www.regulations.doe.gov/ccms.

May 2013