CHILDREN'S ONLINE PRIVACY P

Background and Summary

The Children's Online Privacy Protection Act of 1998 (COPPA) (15 USC 6501 et seq.) addresses the collection, use, or disclosure of personal information about children that is collected from children through websites or other online services. On November 3, 1999, the Federal Trade Commission (FTC) issued a regulation (16 CFR 312), which implements COPPA. The regulation became effective on April 21, 2000.

Financial institutions are subject to COPPA if they operate a website(s) or online service(s) (or portion thereof) directed to children, or have actual knowledge that they are collecting or maintaining personal information from a child online. COPPA grants each of the federal financial regulatory agencies enforcement authority over the institutions they supervise under 12 USC 1818.

Definitions

The terms "child" or "children" mean individuals under the age of 13.

The term "personal information" means individually identifiable information about an individual collected online, including first and last name, home address, e-mail address, telephone number, social security number, or any combination of information that permits physical or online contact.

COPPA employs several other definitions including "communication," "disclosure" and "verifiable parental consent." For the complete listing of definitions see 16 CFR 312.2.

The following examination procedures should be consulted when examining an institution for whom any part of the company's website is directed to or captures information from children. At the close of the exam procedures, you will find the General Requirements of the COPPA regulation as well as a brief synopsis of the specific regulatory sections (e.g. Content, Notice to a Parent, Placement of Notice on website). Finally, the last document in this section is a COPPA Worksheet, a numbered checklist, to be used at the close of this particular section of the examination.

INITIAL PROCEDURES

1. From direct observation of the institution's website or online service and through discussions with appropriate management officials, ascertain whether the financial institution is subject to COPPA by determining if it operates a website(s) or online service(s) that:

   - Is directed to children; or

- Knowingly collects or maintains personal information from children. A thrift knowingly collects or maintains information from a child when it requests age or birth date information on its website and persons under age 13 can and do respond by providing age or birth date combined with other individually identifiable information.

If the institution does not currently operate a website directed to children or knowingly collects information about them, the institution is not subject to COPPA and no further examination procedures are necessary.

2. If the institution is subject to COPPA, determine if it is participating in an FTC-approved self-regulatory program. If yes, obtain a copy of the program, and supporting documentation, such as reviews or audits, which demonstrate the institution's compliance with the program. If the self-regulatory authority (SRA) determined that the institution was in compliance with COPPA at the most recent review/audit, or has not yet made a determination, no further examination procedures are necessary. If however, the SRA determined that the institution was not in compliance with COPPA and the institution has not taken appropriate corrective action, complete the remaining procedures.

3. If an institution is subject to COPPA, review applicable audit and compliance program materials to determine whether:

   - Internal review procedures address the COPPA provisions applicable to the institution;
   - The audits or reviews performed were reasonable, accurate and include consideration of issues raised by consumer complaints;
   - Effective corrective action occurred in response to previously identified deficiencies;
   - Deficiencies, their causes, and the effective corrective actions are consistently reported to management or the members of the board of directors; and
   - The frequency of compliance review is appropriate for the level of changes to on-line content.

4. If an institution is subject to COPPA, but does not conduct satisfactory internal audits or compliance reviews, evaluate whether the institution's internal controls are adequate to ensure compliance with COPPA. Consider:

   - Who in the organization is responsible for the institution's compliance with COPPA;
   - Process flowcharts to determine how the institution's COPPAA compliance is planned for, evaluated, and achieved;
   - Policies, procedures and training programs;

- How methods of collecting or maintaining personal information from the website or online service are vetted before implementation;

- How data elements collected from a child are tracked for use and protected;

- Whether data elements collected from a child are disclosed to third parties and how permission for such disclosure is implemented and tracked;

- The resolution process for complaints regarding the treatment of data collected from a child; and

- Any system triggers to alert operations staff about potential COPPA ramifications of web content decisions.

5. Based on the results of the foregoing, determine which verification procedures, if any, should be completed, focusing on the areas of particular risk. The selection of procedures to be employed depends upon the adequacy of the institution's compliance management system and level of risk identified. It may be most efficient to have management conduct any necessary review, correct any self-identified deficiencies and report to the Region a self-assessment of its COPPA compliance.

VERIFICATION PROCEDURES

1. Through testing or management's demonstration of the website or online service, verify that the financial institution does not condition a child's participation in a game, offering of a prize, or another activity on the child's disclosure of more personal information than is reasonably necessary to participate in the activity [16 CFR 312.7].

2. Obtain a sample of data collected on children including data shared with third parties, if applicable, and determine whether:

   - The financial institution has established and maintained reasonable procedures to protect the confidentiality, security and integrity of personal information collected from a child [16 CFR 312.8 and 312.3];

   - Data are collected, used, and shared in accordance with the institution's website notice [16 CFR 312.4 and 312.3]; and

   - Parental permission was obtained prior to the use, collection or sharing of information, including consent to any material change in such practices [16 CFR 312.5(a)].

3. Through testing or management's demonstration of the website or online service and a review of a sample of parental consent forms or other documentation determine whether the financial

institution has a reasonable method for verifying the person providing the consent is the child's parent [16 CFR 312.5 (b)(2)].

4. Review a sample of parent requests for personal information provided by their children and verify that the financial institution:

   - Provided, upon request, a description of the specific types of personal information collected [16 CFR 312.6(a)(1)];

   - Complied with a parent's instructions concerning the collection or disclosure of their child's information. [16 CFR 312.6(a)(2)];

   - Allowed parents to review any personal information collected from the child [16 CFR 312.6(a)(3)]; and

   - Verified that persons requesting information are parents of the child [16 CFR 312.6 (a)(3)].

5. Complete the COPPA Worksheet on access, clarity and content of electronic notices on the thrift's website or online service. (see "Attachment A").

CONCLUSIONS

1. Summarize all findings, supervisory concerns and regulatory violations.

2. For the violation(s) above, determine the root cause by identifying weaknesses in internal controls, audit and compliance reviews, training, management oversight, or other factors; also, determine whether the violation(s) are repetitive or systemic.

3. Identify action needed to correct violations and weaknesses in the institution's compliance system.

4. Discuss findings with the institution's management and obtain a commitment for corrective action.

General Requirements of the COPPA Regulations

The regulation requires an operator of a website or online service directed to a child, or any operators who have actual knowledge that they are collecting or maintaining personal information from a child, to:

- Provide a clear, complete and understandably written notice on the website or online service of their information collection practices with regard to children, describing how the operator collects, uses and discloses the information (16 CFR 312.4);

- Obtain, through reasonable efforts and with limited exceptions, verifiable parental consent prior to the collection, use or disclosure of personal information from children (16 CFR 312.5);

- Provide a parent, upon request, with the means to review the personal information collected from his/her child and to refuse to permit its further use or maintenance (16 CFR 312.6);

- Limit collection of personal information for a child's online participation in a game, prize offer, or other activity to information that is reasonably necessary for the activity (16 CFR 312.7); and

- Establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of the personal information collected from children (16 CFR 312.8).

Placement of Notice on the Website [16 CFR 312.4(b)(1)]

An operator of a website or online service directed to children must post a link to a statement describing how it collects, uses and discloses information from and about any child on its homepage and everywhere on the site or service where it collects personal information from any child. An operator of a general audience website that has a separate children's area must post a link on the home page of the children's area.

These links must be placed in a clear and prominent place on the home page of the website or online service. To make a link clear and prominent, a financial institution may, for example, use a larger font size in a different color on a contrasting background. A link in small print at the bottom of a home page does not satisfy the clear and prominent guidelines.

Content [16 CFR 312.4(b)(2)]

The notice must state among other requirements:

- The name, address, telephone number and e-mail address of all operators collecting or maintaining personal information from any children through the website or online service;

- The types of personal information collected from any children and how the information is collected;

- How the operator uses the personal information;

- Whether the operator discloses information collected to third parties. If it does, the notice must state the types of businesses engaged in by the third parties, the purposes for which the information is used, and whether the third parties have agreed to maintain the confidentiality, security and integrity of the information. In addition, the notice must state that the parent has the option to consent to the collection and use of the information without consenting to the disclosure of the information to third parties;

- That the operator may not require as a condition of participation in an activity that a child disclose more information than is reasonably necessary to participate in such activity; and

- That a parent can review his or her child's personal information, have it deleted, and refuse to allow any further collection or use of the child's information, and state the procedures for doing so.

Notice to a Parent [16 CFR 312.4 (c)]

An operator is required to obtain verifiable parental consent before any collection, use or disclosure of personal information from any children. An operator also must make reasonable efforts to provide a parent with notice of the operator's information practices with regard to children, as described above, and in the case of a notice seeking consent, the following additional information:

- The operator wishes to collect personal information from the parent's child;
- The parent's consent is required for the collection, use and disclosure of the information; and
- How the parent can provide consent.

Methods for Obtaining Parental Consent [16 CFR 312.5 (b)]

Until April 2002, the FTC will use a sliding scale approach for obtaining parental consent in which the required method of consent will vary based on how the financial institution intends to use the child's personal information. If the information is used for internal purposes, which may include an operating subsidiary or affiliate, a less rigorous method of consent is required. If the financial institution discloses the information to others, the child's privacy is at greater risk, and a more reliable method of consent is required. Anticipating that technical developments soon will allow companies to use more reliable methods to verify identities, the FTC expects to phase out the sliding scale approach by April 2002, subject to an FTC review planned for October, 2001.

Internal Uses

Financial institutions that use the personal information internally may use e-mail to get parental consent provided the operator takes additional steps to verify that a parent is the person providing consent, such as by confirming receipt of consent by e-mail, letter, or telephone call.

Disclosure to Others

Disclosure of a child's personal information to others (e.g., chat rooms, message boards, and third parties) presents greater risk to a child's privacy, and the FTC's sliding scale approach noted above, requires a more reliable method of consent, including:

- Obtaining a signed consent form from a parent via postal mail or facsimile;
- Accepting and verifying a credit card number;
- Taking a parent call, through a toll-free telephone number staffed by trained personnel;

- E-mail accompanied by digital signature; or
- E-mail accompanied by a PIN or password obtained through one of the methods mentioned above.

Disclosures to Third Parties

A parent may permit an operator of a website or online service to collect and use information about a child while prohibiting the operator from disclosing the child's information to third parties. An operator must give a parent this option.

Parental Consent to Material Changes [16 CFR 312.5(a)]

The operator must send a new notice and request for consent to a parent if there are material changes in the collection, use or disclosure practices to which a parent has previously agreed.

Exceptions to Prior Parental Consent Requirement [16 CFR 312.5(c)]

A financial institution does not need prior parental consent when it is collecting:

- A parent's or child's name or online contact information solely to obtain consent or to provide notice. If the operator has not obtained parental consent after a reasonable time from the date of the information collection, the operator must delete such information from its records;
- A child's online contact information solely to respond on a one-time basis to a specific request from the child, if the information is not used to recontact the child, and is deleted by the operator;
- A child's e-mail address to respond more than once to a specific request of the child (e.g., a request to receive a monthly online newsletter), when the operator does not use the information to contact the child beyond the scope of the request, and a parent is notified and allowed to request that the information not be used further;
- The name and online contact information of the child to be used solely to protect the child's safety; or
- The name and online contact information of the child solely to protect the security of the site, to take precautions against liability, or to respond to judicial process, law enforcement agencies, or an investigation related to public safety.

Right to Review Information [16 CFR 312.6]

An operator of a website or online service is required to provide a parent with a means to obtain any personal information collected from his or her child. At a parent's request, an operator must provide a parent with:

- A description of the types of personal information it has collected from the child; and
- An opportunity to review the information collected from the child.

Before a parent can review a child's information, the operator must take steps to ensure that the person making the request is the child's parent. An operator or its agent will not be held liable under any federal or state laws for any disclosures made in good faith and following reasonable procedures to verify a requester's identity in responding to a request for disclosure of personal information.

The regulations allow parents to refuse to permit an operator to continue to use or to collect their child's personal information in the future and to instruct the operator to delete the information. If a parent does so, an operator may terminate its service to that child.

Confidentiality, Security and Integrity of Personal Information Collected from a Child [16 CFR 312.8]

The operator of a website or an online service is required to establish and maintain reasonable procedures to protect the confidentiality, security and integrity of personal information collected from any children. Operators must have adequate policies and procedures for protecting a child's personal information from loss, misuse, unauthorized access or disclosure. Operators are allowed to select an appropriate method for implementing this provision.

Safe-harbor [16 CFR 312.10]

Industry groups, financial institutions or others may establish, with the FTC's approval, a self-regulatory program. An operator of a website or online service that complies with FTC-approved self-regulatory guidelines will receive a "safe harbor" from the requirements of COPPA and the regulations. Self-regulatory guidelines must require that a website and an online service implement substantially similar requirements that provide the same or greater protections for a child as the FTC regulations (16 CFR 312.2-9). These guidelines also must include an effective, mandatory mechanism for assessing operators' compliance, as well as incentives to ensure that an operator will comply.

Attachment A

CHILDREN'S ONLINE PRIVACY PROTECTION ACT WORKSHEET FOR NOTICES

Website Notice (16 CFR 312.4)	Yes	No
1. A link is posted on the website to a notice of the financial institution's information practices with regard to children. [16 CFR 312.4 (b)].		
2. The link to the notice is clearly labeled as a notice of the website's information practices with regard to children, and is placed in a clear and prominent place on the home page of the website and at each area on the website where a child directly provides personal information [16 CFR 312.4(b)(1)].		
3. The notice states:		
• The name, address, telephone number, and e-mail address of any operator who collects or maintains personal information from a child through the website [16 CFR 312.4(b)(2)(i)];		
• The types of information collected from a child and whether the information is collected directly or passively [16 CFR 312.4(b)(2)(ii)];		
• How such information is or may be used [16 CFR 312.4(b)(2)(iii)];		
• Whether such information is disclosed to a third party and, if so, determine whether:		
- The notice states the types of businesses engaged in by the third parties;		
- The purposes for which the information is used;		
- The third parties have agreed to maintain the confidentiality, security and integrity of the information; and		
- That a parent has the option to consent to the collection and use of the information without consenting to the disclosure; [16 CFR 312.4(b)(2)(iv)];		
• The operator is prohibited from conditioning a child's participation in an activity on the disclosure of more information than is reasonably necessary to participate in such activity [16 CFR 312.4(b)(2)(v)]; and		
• A parent can review and have deleted the child's personal information; and		
- Refuse to permit further collection or use of the child's information; and		
- States the procedures for doing so [16 CFR 312.4(b)(2)(vi)].		

	Yes	No
4. The notice to a parent		
• States that the operator wishes to collect information from the child.		
• Includes the information contained in the §312.4(b) website notice (see step 3 above) [16 CFR 312.4(c)(1)(i).		
• If §312.5(a) applies, states that the parent's consent is required for the collection, use and/or disclosure of such information and states the means by which the parent can provide verifiable consent to the collection of information. [16 CFR 312.4(c)(1)(ii).		
• Includes additional information as detailed in the regulation if the exceptions in §312.5(c)(3) and (4) apply.		