Children's Online Privacy Protection Act

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.

General Requirements

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 (§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 (§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 (§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 (§312.7)

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

Children's Online Privacy Protection Act

Notice on the Website

Placement of Notice

An operator of a website or online service directed to children must post a link to a notice of its information practices with regard to children 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 to its notice 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 or a link that is indistinguishable from other adjacent links does not satisfy the clear and prominent guidelines.

Content of the Notice

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, or the same information for one operator who will respond to all inquiries and the names of all the above operators

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

- How the operator uses or may use 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

- 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.

Children's Online Privacy Protection Act

Notice to a Parent

Content of the Notice

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
- How the parent can provide consent.

Parental Consent and Review of Information

Methods for Obtaining Parental Consent
Before collecting, using, or disclosing personal information from a child, an operator must obtain verifiable parental consent from the child's parent. Methods for obtaining such consent include the following:

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

However, until April 21, 2005, the regulation permits 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 eventually will allow companies to use more reliable methods to verify identities, the regulation phases out the sliding scale approach by April 15, 2005 subject to a FTC review planned in 2005.

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. Operators who use such methods must provide notice that the parent can revoke consent.

Children's Online Privacy Protection Act

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 under the FTC's sliding scale approach, would require a method of consent more reliable than those for internal uses. These more reliable methods of consent include those listed in the bullet points above.

Parent Permitted 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

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

Exceptions to Prior Parental Consent Requirement

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 re-contact the child, and is deleted by the operator

- A child's online contact information to respond more than once to a specific request of the child (e.g., a request to receive a monthly online newsletter), when the 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

- 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.

Parents' Right to Review Information

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 regulation allows 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.

Other Requirements

Confidentiality, Security and Integrity of Personal Information Collected from a Child

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 child.

Safe-harbor

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 regulation. 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 sections 312.2 through 312.9 of the regulation. These guidelines also must include an effective, mandatory mechanism for assessing operators' compliance, as well as incentives to ensure that an operator will comply.

Children's Online Privacy Protection Act

Examination Objectives

1. To assess the quality of a financial institution's compliance management policies and procedures for implementing COPPA, specifically ensuring consistency between its notices about its policies and practices and what it actually does.

2. To determine the reliance that can be placed on a financial institution's internal controls and procedures for monitoring the institution's compliance with COPPA.

3. To determine a financial institution's compliance with COPPA, specifically in meeting the following requirements:

   - Providing 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

   - Obtaining, through reasonable efforts and with limited exceptions, verifiable parental consent prior to the collection, use, or disclosure of personal information from children

   - Providing 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

   - Complying with any direction or request of a parent concerning his or her child's information

   - Limiting 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

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

4. To initiate effective corrective actions when violations of law are identified, or when policies or internal controls are deficient.

Children's Online Privacy Protection Act

Examination Procedures

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
   - Knowingly collects or maintains personal information from children.

Stop here if the institution does not currently operate a website that is directed to children or knowingly collects information about them, the institution is not subject to COPPA and no further examination for COPPA is necessary.

2. Determine if the institution is participating in a 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 for COPPA is necessary. On the other hand, if the SRA determined that the institution was not in compliance with COPPA and the institution has not taken appropriate corrective action, continue with the procedures below.
   - If the institution is not participating in a FTC-approved, self-regulatory program, continue with the procedures below.

3. Determine, through a review of available information, whether the institution's internal controls are adequate to ensure compliance with COPPA. Consider the following:

   - Organization chart to determine who is responsible for the institution's compliance with COPPA
   - Process flowcharts to determine how the institution's COPPA compliance is planned for, evaluated, and achieved
   - Policies and procedures
   - Methods of collecting or maintaining personal information from the website or online service
   - List of data elements collected from any children and a description of how the data are used and protected

- List of data elements collected from any children that are disclosed to third parties and any contracts or agreements governing the use of that information with those third parties
- Complaints regarding the treatment of data collected from a child
- Internal checklists, worksheets, and other review documents.

4. Review applicable audit and compliance review material, including work papers, checklists, and reports, to determine whether:
   - The procedures address the COPPA provisions applicable to the institution
   - Effective corrective action occurred in response to previously identified deficiencies
   - The audits and reviews performed were reasonable and accurate
   - Deficiencies, their causes, and the effective corrective actions are consistently reported to management or the members of the board of directors
   - The frequency of the compliance review is satisfactory.
5. Review a sample of complaints that allege the inappropriate collection, sharing, or use of data from a child to determine whether there are any areas of concern, as available.
6. Based on the results of the foregoing, determine the depth of review focusing on the areas of particular risk. The procedures to be employed depend upon the adequacy of the institution's compliance management system and level of risk identified.

Verification Procedures

1. Review the notice of the financial institution's information practices with regard to children to determine whether it is clearly and prominently placed on the website and contains all information required by the regulation (§312.4).
2. Obtain a sample of data collected from any 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 [§312.8 and 312.3]
   - Data are collected, used, and shared in accordance with the institution's website notice [§312.4 and 312.3]

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

- Data are collected, used, and shared in accordance with parental consent [§§312.5 and 312.6]

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 [§312.5 (b)(2)].

4. Review a sample of parental 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 [§312.6(a)(1)]

    - Complied with a parent's instructions concerning the collection, use, maintenance, or disclosure of their child's information. [§312.6(a)(2)]

    - Allowed a parent to review any personal information collected from the child [§312.6(a)(3)]

    - Verified that the person requesting information is a parent of the child [§312.6 (a)(3)].

5. 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 [§312.7].

Conclusions

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

2. For the violation(s), 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.

Children's Online Privacy Protection Act

Children's Online Privacy Protection Act Worksheet for Website Notices	Yes	No
Notice on the Website 1. Does the institution knowingly collect or maintain personal information from a child in a manner that violates the regulation? [§312.3] 2. Is the link to the notice clearly labeled as a notice of the website's information practices with regard to children, and is it 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 or is asked to provide personal information? [§312.4(b)(1)] 3. Does the notice state: • 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, or the same information for one operator who will respond to all inquiries along with the names of all operators [§312.4(b)(2)(i)] • The types of information collected from a child and whether the information is collected directly or passively [§312.4(b)(2)(ii)] • How such information is or may be used [§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 ✓ A parent has the option to consent to the collection and use of the information without consenting to the disclosure; ✓ [§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 [§312.4(b)(2)(v)]; and A parent can review and have deleted the child's personal information; and can refuse to permit further collection or use of the child's information; and is provided with the procedures for doing so [§312.4(b)(2)(vi)].		

Children's Online Privacy Protection Act

Children's Online Privacy Protection Act Worksheet for Website Notices	Yes	No
Notice to a Parent 5. Does the institution make reasonable efforts to ensure that a parent of the child receives the notice? [§312.4(c)] 6. Does the notice to the parent state: • That the operator wishes to collect information from the child [§312.4(c)(1)(i)(A)] • The information contained in the notice of it information practices regarding children on its website [§312.4(b)(2), §312.4(c)(1)(i)(B)] • 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 [§312.4(c)(1)(ii)] • If the collection of information is to respond directly more than once to a specific request from the child, the notice must state that: ✓ The operator has collected the child's online contact information to respond to the child's request for information and that the requested information will require more than one contact with the child ✓ The parent may refuse to permit further contact with the child and require the deletion of the information, and how the parent can do so ✓ If the parent fails to respond to the notice, the operator may use the information for the purpose(s) stated in the notice. [§312.4 (c)(1)(iii)] • If the collection of information is to protect the safety of the child, the notice must state that: ✓ The operator has collected the child's name and online contact information to protect the safety of the child ✓ The parent may refuse to permit further contact with the child and require the deletion of the information, and how the parent can do so ✓ If the parent fails to respond to the notice, the operator may use the information for the purpose(s) stated in the notice. [§312.4 (c)(1)(iv)]		
Parental Consent 7. Does the institution obtain consent of the parent prior to any collection, use, or disclosure of personal information from any children, outside of the exceptions named in §312.5(c)? [§312.5(a)(1)] 8. If changes to the policy on collecting, using, or disclosing data on children occurred, does the institution request and review updated consent forms or documentation and determine whether parental permission is still in effect? [§312.5(a)] 9. Does the institution have a reasonable method for verifying the person providing the consent is the child's parent? [§312.5(b)(2)]		

Children's Online Privacy Protection Act

Children's Online Privacy Protection Act Worksheet for Website Notices	Yes	No
Right of Parent to Review Personal Information Provided by a Child 10. Does the institution respond to parental requests to review information provided by their children by providing: • A description of the specific types of personal information collected [§312.6(a)(1)] • The opportunity for the parent to refuse to permit the further use or collection of personal information and to direct the financial institution to delete the child's personal information [§312.6(a)(2)] • A procedures for reviewing any personal information collected for the child d [§312.6(a)(3)] • Adequate procedures to ensure those persons requesting information are parents of the child in question. [§312.6(a)(3)]		
Prohibition Against Conditioning a Child's Participation on Collection of Personal Information 11. Does the operator refrain from conditioning a child's participation in a game, the offering of a prize or another activity on the child's disclosing more personal information than necessary to participate? [§312.7]		
Confidentiality Security and Integrity of Personal Information Collected from a Child 12. Does the institution maintain reasonable policies and procedures for protecting a child's personal information from loss, misuse, unauthorized access or disclosure? [§312.8]		