Children's Online Privacy Protection Act

Background

Financial institutions that operate one or more web sites or online services directed at children (or a portion of such a web site or service), or that have knowledge that they are collecting or maintaining personal information from a child online, are subject to certain regulatory requirements. Those requirements, which are set forth in the Children's Online Privacy Protection Act of 1998 (COPPA) (15 USC 6501 et seq.), address the collection, use, and disclosure of personal information about children collected from children through web sites or other online services. The regulation that implements COPPA (16 CFR 312) was issued in November 1999 by the Federal Trade Commission and became effective in April 2000. Each of the federal financial regulatory agencies has enforcement authority for COPPA over the institutions it supervises.

Definitions

- *Child (children)*—An individual (individuals) under the age of 13
- *Operator*—Any person who operates a web site located on the Internet or an online service and who collects or maintains personal information from or about the users of, or visitors to, such a web site, or on whose behalf such information is collected or maintained where the web site or online service is used for commercial purposes
- *Personal information*—Individually identifiable information about an individual collected online, including first and last names, home address, e-mail address, telephone number, Social Security number, or any combination of information that permits physical or online contact

General Requirements

Operators of web sites or online services directed at children, and operators who have knowledge that they are collecting or maintaining personal information from children, are required to

- Provide, on the web site or online service, a clear, complete, and understandable written notice of 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 before collecting, using, or disclosing personal information from children (§ 312.5)
- Provide a parent, upon request, with the means of reviewing the personal information collected from his or her child and of refusing to permit the information's further use or maintenance (§ 312.6)
- Limit collection of personal information for the purpose of facilitating a child's online participation in a game, prize offer, or other activity to that 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)

Notice on Web Site

Placement of Notice

An operator of a web site or online service directed at children must post, on its home page and everywhere on the site or service where it collects personal information from any child, a link taking viewers to a notice of its information practices with regard to children. An operator of a general-audience web site that has a separate children's area must post a link to its notice on the home page of the children's area.

Such links must be placed in a clear and prominent place on the home page of the web site or online service. To make the link clear and prominent, an operator 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 adjacent links does not satisfy the ''clear and prominent'' guidelines.

Content of Notice

The web site notice must, among other requirements, state

- The name, address, telephone number, and e-mail address of all operators collecting or maintaining personal information from children through the web site or online service; or the same information for one operator who will respond to all inquiries, in addition to the names of all the operators
- The types of personal information collected from 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 business engaged in by the third parties
  - The purposes for which the information is used
  - Whether the third parties have agreed to maintain the confidentiality, security, and integrity of the information
  - That the parent has the option of consenting 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 the activity
- That a parent may 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. Procedures for parental review, deletion, and refusal to allow further collection or use must also be included in the notice.

Notice to Parent

Content of Notice

An operator is required to obtain verifiable parental consent before collecting, using, or disclosing personal information from children. An operator must also 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, must state the following:

- That the operator wishes to collect personal information from the parent's child
- That 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 of Obtaining Parental Consent

Obtaining verifiable parental consent may be done by any of several methods. Currently, operators may take a ''sliding-scale'' approach whereby the method of obtaining parental consent depends on how the financial institution intends to use the child's personal information.

Under the sliding-scale approach, if the information is to be used solely for internal purposes (including use by an operating subsidiary or an affiliate), the required method of obtaining consent is less rigorous. A financial institution that uses the information internally may obtain parental consent via e-mail, provided that the operator takes additional steps to verify that the person providing consent is in fact the child's parent by, for example, confirming receipt of consent by e-mail, letter, or telephone call. Operators who use such methods must provide notice that the parent may revoke consent.

The sliding-scale approach was adopted in anticipation that technical developments would eventually allow the use of more-reliable methods to verify identities. This approach, which was originally scheduled to be phased out by April 15, 2005, has been extended indefinitely by the FTC.

If, in contrast, the information is to be disclosed to others (for example, to chat rooms, message boards, or third parties), putting the child's privacy at greater risk, a more-reliable method of consent is required. These more-reliable methods include

- Obtaining a signed consent form from a parent via mail or fax
- Accepting and verifying a credit card number
- Taking a call from a parent, through a toll-free telephone number staffed by trained personnel
- Receiving e-mail accompanied by a digital signature
- Receiving e-mail accompanied by a PIN or password obtained through one of the verification methods described in the bullet items above

Parent-Permitted Disclosures to Third Parties

A parent may permit an operator of a web site 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

An 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 the parent has previously agreed.

Exceptions to Prior-Parental-Consent Requirement

A financial institution does not need prior parental consent to collect

- 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 in a reasonable time after the information was collected, the operator must delete the 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. In such an instance, the contact information must not be used to re-contact the child and must be deleted.
- A child's online contact information to respond more than once to a specific request made by the child (for example, a request to receive a monthly online newsletter), if the parent is notified and allowed to request that the information not be used in any other way
- 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

Parental Right to Review Information

An operator of a web site or online service is required to provide a parent with a means of obtaining any personal information collected from his or her child. At a parent's request, the operator must provide the 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 is permitted to 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 after having followed reasonable procedures to verify the requester's identity.

Parents may refuse to permit an operator to continue to use or collect a child's personal information in the future and may instruct the operator to delete the information. If a parent does so, the 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 web site or an online service is required to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from a child. Operators must have adequate policies and procedures for protecting a child's personal information from loss, misuse, unauthorized access, or disclosure. Operators are permitted to select an appropriate method for implementing this provision.

Safe Harbor

With prior FTC approval, industry groups, financial institutions, and others may establish a self-regulatory program. Web site operators and online services that comply with FTC-approved self-regulatory guidelines will receive a ''safe harbor'' from the requirements of COPPA and the regulation. Self-regulatory guidelines must require the implementation of substantially similar requirements that provide the same or greater protections for a child as sections 312.2 through 312.9 of the regulation. The guidelines must also 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 and Procedures

EXAMINATION OBJECTIVES

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

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

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

   - Providing, on the web site or online service, a clear, complete, and understandable written notice of its information-collection practices with regard to children that describes 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 of reviewing the personal information collected from his or her child and the means with which to refuse 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

EXAMINATION PROCEDURES

Initial Procedures

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

   - Is directed at children
   - Knowingly collects or maintains personal information from children

Note: Stop here if the institution does not currently operate a web site that is directed to children or does not knowingly collect information about children. In these cases the institution is not subject to COPPA, and no further examination for COPPA is necessary.

2. Determine if the financial institution is participating in an FTC-approved self-regulatory program.

   - If it is, obtain a copy of the program and supporting documentation, such as reviews or audits, that demonstrate the financial institution's compliance with the program. If the self-regulatory authority (SRA) determined that the financial institution was in compliance with COPPA at the most recent review or audit or has not yet made a determination, no further examination for COPPA is necessary. If, on the other hand, the SRA determined that the institution was not in compliance with COPPA and the institution has not taken appropriate corrective action, continue with the remaining procedures.
   - If the financial institution is not participating in a FTC-approved self-regulatory program, continue with the remaining procedures.

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

   - Organization chart, to determine who is responsible for the financial institution's compliance with COPPA

- Process flowcharts, to determine how the institution's COPPA compliance is planned for, evaluated, and achieved
- Policies and procedures that relate to COPPA compliance
- Methods of collecting or maintaining personal information from the web site 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 with those third parties governing the use of that information
- 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 workpapers, 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 members of the board of directors
   - The frequency of the compliance review is satisfactory
5. Review, as available, 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.
6. Based on the results of the foregoing, determine the depth of the examination review, focusing on the areas of particular risk. The procedures to be employed depend on the adequacy of the institution's compliance management system and the level of risk identified.

Verification Procedures

1. Review the notice describing the financial institution's information practices with regard to children to determine whether it is clearly and prominently placed on the web site and contains all information required by the regulation. (§ 312.4)
2. Obtain a sample of data collected from children, including data shared with third parties, if applicable, and determine whether
   - The institution has established and maintained reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from a child (§§ 312.3 and 312.8)
   - Data are collected, used, and shared in accordance with the institution's web site notice (§§ 312.3 and 312.4)
   - 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 web site or online service and a review of a sample of parental consent forms or other documentation, determine whether the institution has a reasonable method for verifying that 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 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 his or her 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 web site or online service, verify that the 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. Determine the root cause of any violations by identifying weaknesses in internal controls, audit and compliance reviews, training, manage-

ment oversight, or other factors; also, determine whether the violations are repetitive or systemic.

3. Identify any action needed to correct violations and weaknesses in the financial 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
Worksheet

Notice on Web Site

1. Does the financial institution knowingly collect or maintain personal information from a child in a manner that violates the regulation? (§ 312.3) Yes No
2. Is the link to the notice clearly labeled as a notice of the web site's information practices with regard to children, and is it placed in a clear and prominent place on the home page of the web site and at each area on the web site where a child directly provides or is asked to provide personal information? (§ 312.4(b)(1)) Yes No
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 web site 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)) Yes No
   - The types of information collected from a child, and whether the information is collected directly or passively (§ 312.4(b)(2)(ii)) Yes No
   - How such information is or may be used (§ 312.4(b)(2)(iii)) Yes No
   - Whether such information is disclosed to third parties. If it is, determine whether the notice states
     – The types of businesses engaged in by the third parties Yes No
     – The purposes for which the information is used Yes No
     – That the third parties have agreed to maintain the confidentiality, security, and integrity of the information Yes No
     – That a 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 (§ 312.4(b)(2)(iv)) Yes No
   - That 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)) Yes No
   - That a parent may review and have deleted the child's personal information, may 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)) Yes No

Notice to a Parent

4. Does the financial institution make reasonable efforts to ensure that a parent of the child receives the notice? (§ 312.4(c)) Yes No
5. Does the notice to the parent state
   - That the operator wishes to collect information from the child (§ 312.4(c)(1)(i)(A)) Yes No
   - The institution's practices regarding children, as noted on its web site (§§ 312.4(b)(2) and 312.4(c)(1)(i)(B)) Yes No
   - That the parent's consent is required for the collection, use, and disclosure of such information, and the means by which the parent can provide verifiable consent to the collection of information (§ 312.4(c)(1)(ii)) Yes No

- If the operator has collected information from a child that will be used to respond directly more than once to a specific request from the child, does the notice 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 Yes No
  - That 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 Yes No
  - That 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)) Yes No
- If the purpose behind the collection of information is to protect the safety of the child, does the notice state
  - That the operator has collected the child's name and online contact information to protect the safety of the child Yes No
  - That 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 Yes No
  - If the parent fails to respond to the notice, that the operator may use the information for the purpose(s) stated in the notice (§ 312.4(c)(1)(iv)) Yes No

Parental Consent

6. Does the financial institution obtain the consent of the parent prior to any collection, use, or disclosure of personal information from any children, outside the exceptions listed in section 312.5(c)? (§ 312.5(a)(1)) Yes No
7. 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)) Yes No
8. Does the institution have a reasonable method for verifying that the person providing the consent is the child's parent? (§ 312.5(b)(2)) Yes No

Right of Parent to Review Personal Information Provided by a Child

9. Does the financial 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)) Yes No
   - 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)) Yes No
   - Procedures for reviewing any personal information collected from the child (§ 312.6(a)(3)) Yes No
   - Adequate procedures to ensure that those persons requesting information are parents of the child in question (§ 312.6(a)(3)) Yes No

Prohibition against Conditioning a Child's Participation on Collection of Personal Information

10. 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 disclosure of more personal information than necessary to participate? (§ 312.7) Yes No

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

11. Does the financial institution maintain reasonable policies and procedures for protecting a child's personal information from loss, misuse, unauthorized access, or disclosure? (§ 312.8)	Yes	No