RESCINDED

OCC 2002-31

Subject: Children's Online Privacy Protection Act (COPPA)
Date: July 16, 2002

To: Chief Executive Officers and Compliance Officers of All National Banks, Department and Division Heads, and All Examining Personnel

Description: Examination Procedures

and will not be subject to COPPA examinations by the OCC. However, financial institutions are urged to review their Web sites and their online information collection practices to ensure that they do not inadvertently trigger the provisions of this act.

The Federal Trade Commission issued a regulation, 16 CFR 312, implementing COPPA. It became effective on April 21, 2000.

For more information, contact your supervisory office or the Compliance Department at (202) 874-4428.

David G. Hammaker
Deputy Comptroller for Compliance

Related Links

- COPPA Examination Procedures

CHILDREN'S ONLINE PRIVACY PROTECTION ACT

Children's Online Privacy Protection Act

Table of Contents

Children's Online Privacy Protection Act

Introduction

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 that is collected from children through Web sites 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 Web site(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.

Financial institutions that do not currently operate a Web site or online service directed to children, or do not have actual knowledge that they are collecting or maintaining personal information from a child online, are not subject to COPPA and will not be subject to COPPA examinations by the Office of the Comptroller of the Currency (OCC). However, financial institutions are urged to review their Web sites and their online information collection practices to ensure that they do not inadvertently trigger the provisions of this Act.

Definitions

"Child", "Children": (an) individual(s) under the age of 13.

"Personal information": 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 Web site 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 to the parent and on the Web site 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 and have deleted the personal information collected from his or 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).

Notice on the Web Site

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

An operator of a Web site or online service directed to children must post a link to a notice of its information practices with regard to children on its home page and at each area on the site or service where it collects personal information from any child. 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.

These links must be placed in a clear and prominent location on the home page of the Web site 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 that requires visitors to scroll down the 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 child through the Web site or online service;

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

- The way the operator uses, or may use, the personal information;

- A statement of 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 there is a prohibition against requiring, 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 has a right to 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 child can be made. 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's wishes to collect personal information from the parent's child;

- The requirement of the parent's consent for the collection, use, and disclosure of the information; and

- The way(s) the parent can provide consent.

Internal Uses [16 CFR 312.5(b)]

Financial institutions that use the personal information solely for internal purposes 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.

Disclosure to Others [16 CFR 312.5(b)]

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 requires a more reliable method of consent. The method used to obtain verifiable parental consent must be reasonably calculated, in light of available technology, to ensure that the person providing the consent is the child's parent. Methods that satisfy this requirement include:

- Obtaining a signed consent form from a parent via postal mail or facsimile;

- Accepting and verifying a parent's credit card number;

- Taking a parent's call, through a toll-free telephone number staffed by trained personnel;

- Receiving a parent's e-mail, accompanied by a digital signature; and

- Receiving an e-mail from a parent that is accompanied by a personal identification number (PIN) or password obtained through one of the methods mentioned above.

Disclosures to Third Parties [16 CFR 312.5(a)]

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 [16 CFR 312.5(a)]

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 [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 period 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 to, on a one-time basis, 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 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 Web site or online service is required to provide to a parent a means by which he or she can obtain any personal information collected from his or her child by that operator. 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. These methods might include requiring a parent to use a credit card in connection with a transaction; having a parent call a toll-free number staffed by trained personnel; using a digital certificate that uses public key technology; or using e-mail accompanied by a PIN or password.

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 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 any child.

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 Web site or online service that complies with FTC-approved, self-regulatory guidelines will receive a "safe harbor" from the requirements of COPPA and the regulation.

To be approved by the FTC, self-regulatory guidelines must include a requirement that operators subject to the guidelines implement substantially similar requirements that provide the same or greater protections for a child as the FTC regulation (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.

General Procedures

Objective: Determine the scope of the Children's Online Privacy Protection Act (COPPA) examination.

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

   - Is directed to children; or
   - Knowingly collects or maintains personal information from children.

   If the institution does not currently operate a Web site directed to children or knowingly collect information about them, the institution is not subject to COPPA, and no further examination for COPPA is necessary.

2. If the institution is subject to COPPA, determine whether it is participating in an FTC-approved, self-regulatory program (see 16 CFR 312.10). If it is, obtain a copy of the program and supporting documentation, such as reviews or audits, that demonstrate the institution's compliance with the program. If, under the self-regulatory program, an independent assessment found the institution in compliance with COPPA, or no assessment has yet been made, no further examination for COPPA is necessary. If, however, the independent assessment found the institution not in compliance with COPPA and the institution has not taken appropriate corrective action, continue with the procedures below.

3. If the institution is subject to COPPA and is not participating in an FTC-approved, self-regulatory program, continue with the procedures below.

4. From the examiner assigned the Compliance Management System program, obtain and review the following information to identify any previous or emerging problems that require follow-up:

   - Historical examination findings.
   - Complaint information from the bank and the OCC's Customer Assistance Group (CAG), and any CAG analytical reports, regarding the inappropriate collection, sharing, or use of data from a child.
   - Significant findings from the compliance audit.
   - Work papers from the prior examination.

5. Determine the following through early discussions with management:

   - Management supervision of compliance with COPPA, including responsiveness to, and corrective measures resulting from, consumer complaint activity.
   - Changes in processes, including forms, contracts, software programs, etc., since the previous examination.
   - Significant changes in policies, personnel, or controls.
   - Internal or external factors that could affect compliance with COPPA.
   - Whether applicable provisions of state laws and regulations are monitored and included in the bank's audit.

6. Complete the "Quality of Risk Management" procedures.

7. Complete appropriate sections of the "Quantity of Risk" procedures. The procedures performed in the "Quantity of Risk" section should address areas of concern identified during the review of "Quality of Risk Management."

8. Complete the "Conclusion Procedures."

Quality of Risk Management

Conclusion: The quality of risk management is (strong, satisfactory, weak).

Policy

Conclusion: The board (has/has not) established appropriate policies to ensure compliance with the Children's Online Privacy Protect Act.

Objective: Determine whether the bank has appropriate formal/informal policies to ensure compliance with COPPA.

1. Determine whether the board has adopted, and management has implemented adequate policies and procedures to maintain compliance with COPPA. Where appropriate, they should address:

   - Significant requirements of the law and the regulation.
   - Responsibilities and accountabilities of key personnel.
   - Training program.
   - Process for responding to changes in the law and the regulation.
   - Role of audit and compliance review.

2. Determine whether the board or an appropriate committee periodically reviews and approves compliance policies.

Processes

Conclusion: Management (has/has not) established effective processes to ensure compliance with COPPA.

Objective: Determine the reliance that can be placed on the bank's processes to prevent violations of COPPA.

1. Determine whether the bank's system for communicating the requirements of, and any subsequent changes to, COPPA is adequate to ensure ongoing compliance.

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

- Organization chart to determine who is responsible for the institution's compliance with COPPA;
- Process flow charts 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 Web site or online service;
- List of data elements collected from a child and a description of how the data are used and protected;
- List of data elements collected from a child that are disclosed to third parties and any contracts or agreements governing the use of that information with those third parties;
- Internal checklists, worksheets, and other review documents.

3. Assess the procedures used to ensure compliance when new online products are developed and operational changes are made.

Personnel

Conclusion: Bank management and personnel (do/do not) possess the required technical skills and knowledge to ensure compliance with COPPA.

Objective: Determine whether bank management and personnel possess sufficient knowledge and technical skills to manage and perform duties related to COPPA.

1. Assess bank management and personnel's knowledge and technical skills regarding COPPA based on conclusions developed while performing these procedures. Also consider:
   - Employee roles and responsibilities.
   - Training and experience.
   - Violations cited.
2. Review the bank's training program (materials, agendas, rosters, frequency, evaluation forms, etc.) and discuss with management to

determine how frequently and how well employees are trained regarding compliance with COPPA.

Controls

Conclusion: Management (has/has not) established effective control systems to ensure compliance with COPPA.

Objective: Determine the reliance that can be placed on the bank's control systems to detect and correct violations of COPPA, including practices and procedures performed by audit and compliance review.

1. Review audit and compliance review material, including working papers and reports, to determine whether:

    - The procedures address the COPPA provisions applicable to the institution;
    - The audits and reviews performed were reasonable and accurate;
    - The frequency of the compliance review is satisfactory;
    - Effective corrective action occurred in response to previously identified deficiencies; and
    - Deficiencies, their causes, and the effective corrective actions are consistently reported to management or the members of the board of directors.

2. Review the following documents and discuss with management to determine whether management information systems are sufficient and whether adequate practices are in place to ensure that timely and appropriate corrective action is taken when weaknesses/violations are identified or when consumer complaints indicate significant deficiencies.

    - Audit/compliance review policies, procedures, and work papers.
    - Audit/compliance review reports and management responses.
    - Management reports.

Quantity of Risk Management

Conclusion: The quantity of risk is (low, moderate, high).

Perform only those procedures identified as areas of concern during the review of the "Quality of Risk Management."

Objective: Determine the bank's level of compliance with COPPA.

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

   - Data are collected, used and shared in accordance with the institution's Web site notice [16 CFR 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 [16 CFR 312.5(a)].

2. Through discussions with management and a review of policies and procedures, determine whether the 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].

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

4. Through testing or management's demonstration of the Web site or online service, verify that the financial institution does not condition 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 is reasonably necessary to participate in the activity [16 CFR 312.7].

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

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

- Complies with a parent's instructions concerning the collection, use, maintenance, or disclosure of his or her child's information. [16 CFR 312.6(a)(2) and 16 CFR 312.4(b)(2)(iv) and (vi)];

- Allows a parent to review any personal information collected from his or her child [16 CFR 312.6(a)(3)]; and

- Verifies that the person requesting information is a parent of the child [16 CFR 312.6 (a)(3)].

6. Complete the "COPPA Worksheet For Notices" by reviewing notices on the Web site or online service.

Conclusions

Objective: Prepare written conclusion summaries, discuss findings with the EIC, and communicate findings to management. If necessary, initiate corrective action when policies or internal controls are deficient or when violations of law or regulation are identified.

1. Summarize findings and violations from the preceding procedural steps to assess the bank's level of compliance with COPPA.

2. For those violations found to be significant or a pattern or practice, determine the root cause of violation(s) by identifying weaknesses in:

   - Internal controls.
   - Audit/independent compliance review.
   - Training.
   - Management oversight.

3. Determine whether a civil money penalty (CMP) or an enforcement action should be recommended (refer to the CMP matrix).

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

5. Form a conclusion about the reliability of the compliance management system for COPPA and provide conclusions to the examiner performing the Compliance Management System program.

6. Determine whether any items identified during this examination could materialize into supervisory concerns before the next on-site examination (considering whether the bank has plans to increase monitoring in the affected area, or anticipates changes in personnel, policy, outside auditors or consultants, or business strategy). If so, summarize your concerns and assess the potential risk to the bank.

7. Determine the impact on the aggregate quantity and direction of risk assessment for any concerns identified during the review. Examiners should refer to guidance provided under the OCC's large and community bank risk assessment programs.

   - Risk categories: compliance, transaction, and reputation risk.
   - Risk conclusions: high, moderate, or low.

- Risk direction: increasing, stable, or declining.

8. Provide, and discuss with, the EIC (and the supervisory office, if appropriate) conclusions, including:

   - A summary of violations and recommended CMPs/enforcement actions, if any.
   - Potential reimbursements.
   - Recommended corrective action.
   - The quantity of risk and quality of risk management.
   - Recommended matters requiring attention (MRA). MRA should cover practices that:
     – Deviate from sound fundamental principles and are likely to result in financial deterioration if not addressed.
     – Result in substantive noncompliance with laws.
   - MRA should discuss:
     – Causative factors contributing to the problem.
     – Consequences of inaction to the institution.
     – Management's commitment for corrective action.
     – The time frame and person(s) responsible for corrective action.

9. Discuss findings with management. Obtain commitment(s) for corrective action as needed. Include in the discussion:

   - The quality of risk management.
   - The quantity of risk (include a listing of all violations, as well as significant violations).
   - MRA(s).

10. As appropriate, prepare a brief comment for inclusion in the report of examination.

11. Prepare a memorandum summarizing work performed (e.g., sampling method used, internal control systems, scope of audit review, conclusions regarding audit, etc.) and update the work program with any information that will facilitate future examinations. Update the OCC database on all violations of law or regulation.

12. Organize and reference working papers in accordance with OCC guidance (PPM 5400-8).

Children's Online Privacy Protection Act Worksheet for Notices

Every "No" answer indicates a potential violation of the regulation or an internal control deficiency and must be fully explained in the work papers.

Web site Notice (16 CFR 312.4)	**Yes**	**No**
1. A Web site link is posted 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 Web site's information practices with regard to children, and is 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 [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 Web site [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 [16 CFR 312.4(b)(2)(iv)]: – 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; • 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 • That 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 – The notice states the procedures for doing so [16 CFR 312.4(b)(2)(vi)].		
4. The notice to a parent • States that the operator wishes to collect information from the child [16 CFR 312.4(c)(1)(i)(A)]. • Includes the information contained in the 16 CFR 312.4(b) Web site notice (see step 3 above) [16 CFR 312.4(c)(1)(i)]. • If 16 CFR 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 16 CFR 312.5(c)(3) and (4) apply.		

Request Letter Enclosure

1. COPPA policies and procedures.

2. COPPA training materials.

3. COPPA compliance reports, audit reports, procedures, and management responses. Note: If the bank participates in an FTC-approved, self-regulatory program, provide a copy of the program and audit reports.

4. Complaints regarding the collection, sharing, or use of data from a child.

5. Copies of Web site notices since the last examination.

6. A list of data elements collected from a child and a description of how the data are used and protected.

7. A list of data elements collected from a child that are disclosed to third parties and any contracts or agreements governing the use of that information with those third parties.

8. A list of parental requests for personal information provided by their children.

9. A description of how parental permission is obtained and the method of verifying that the person providing consent is the child's parent.

Laws

15 USC 6501 et seq., Children's Online Privacy Protection Act

Regulations

16 CFR 312, Children's Online Privacy Protection Rule

OCC Issuances

Bulletin 2001-8, "Guidelines Establishing Standards for Safeguarding Customer Information," dated 02/05/01.

Bulletin 2001-26, "Privacy of Consumer Financial Information; 12 CFR 40," dated 05/25/01.

Bulletin 2001-31, Weblinking," dated 07/03/01.

Bulletin 2001-35, "Examination Procedures to Evaluate Compliance with Guidelines to Safeguard Customer Information," dated 07/18/01.

Advisory Letter 2001-08, "Authentication in an Electronic Banking Environment," dated 07/30/01.

CHILDREN'S ONLINE PRIVACY PROTECTION ACT

Children's Online Privacy Protection Act

Table of Contents

Children's Online Privacy Protection Act

Introduction

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 that is collected from children through Web sites 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 Web site(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.

Financial institutions that do not currently operate a Web site or online service directed to children, or do not have actual knowledge that they are collecting or maintaining personal information from a child online, are not subject to COPPA and will not be subject to COPPA examinations by the Office of the Comptroller of the Currency (OCC). However, financial institutions are urged to review their Web sites and their online information collection practices to ensure that they do not inadvertently trigger the provisions of this Act.

Definitions

"Child", "Children": (an) individual(s) under the age of 13.

"Personal information": 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 Web site 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 to the parent and on the Web site 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 and have deleted the personal information collected from his or 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).

Notice on the Web Site

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

An operator of a Web site or online service directed to children must post a link to a notice of its information practices with regard to children on its home page and at each area on the site or service where it collects personal information from any child. 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.

These links must be placed in a clear and prominent location on the home page of the Web site 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 that requires visitors to scroll down the 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 child through the Web site or online service;

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

- The way the operator uses, or may use, the personal information;

- A statement of 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 there is a prohibition against requiring, 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 has a right to 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 child can be made. 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's wishes to collect personal information from the parent's child;

- The requirement of the parent's consent for the collection, use, and disclosure of the information; and

- The way(s) the parent can provide consent.

Internal Uses [16 CFR 312.5(b)]

Financial institutions that use the personal information solely for internal purposes 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.

Disclosure to Others [16 CFR 312.5(b)]

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 requires a more reliable method of consent. The method used to obtain verifiable parental consent must be reasonably calculated, in light of available technology, to ensure that the person providing the consent is the child's parent. Methods that satisfy this requirement include:

- Obtaining a signed consent form from a parent via postal mail or facsimile;

- Accepting and verifying a parent's credit card number;

- Taking a parent's call, through a toll-free telephone number staffed by trained personnel;

- Receiving a parent's e-mail, accompanied by a digital signature; and

- Receiving an e-mail from a parent that is accompanied by a personal identification number (PIN) or password obtained through one of the methods mentioned above.

Disclosures to Third Parties [16 CFR 312.5(a)]

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 [16 CFR 312.5(a)]

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 [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 period 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 to, on a one-time basis, 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 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 Web site or online service is required to provide to a parent a means by which he or she can obtain any personal information collected from his or her child by that operator. 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. These methods might include requiring a parent to use a credit card in connection with a transaction; having a parent call a toll-free number staffed by trained personnel; using a digital certificate that uses public key technology; or using e-mail accompanied by a PIN or password.

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 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 any child.

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 Web site or online service that complies with FTC-approved, self-regulatory guidelines will receive a "safe harbor" from the requirements of COPPA and the regulation.

To be approved by the FTC, self-regulatory guidelines must include a requirement that operators subject to the guidelines implement substantially similar requirements that provide the same or greater protections for a child as the FTC regulation (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.

General Procedures

Objective: Determine the scope of the Children's Online Privacy Protection Act (COPPA) examination.

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

   - Is directed to children; or
   - Knowingly collects or maintains personal information from children.

   If the institution does not currently operate a Web site directed to children or knowingly collect information about them, the institution is not subject to COPPA, and no further examination for COPPA is necessary.

2. If the institution is subject to COPPA, determine whether it is participating in an FTC-approved, self-regulatory program (see 16 CFR 312.10). If it is, obtain a copy of the program and supporting documentation, such as reviews or audits, that demonstrate the institution's compliance with the program. If, under the self-regulatory program, an independent assessment found the institution in compliance with COPPA, or no assessment has yet been made, no further examination for COPPA is necessary. If, however, the independent assessment found the institution not in compliance with COPPA and the institution has not taken appropriate corrective action, continue with the procedures below.

3. If the institution is subject to COPPA and is not participating in an FTC-approved, self-regulatory program, continue with the procedures below.

4. From the examiner assigned the Compliance Management System program, obtain and review the following information to identify any previous or emerging problems that require follow-up:

   - Historical examination findings.
   - Complaint information from the bank and the OCC's Customer Assistance Group (CAG), and any CAG analytical reports, regarding the inappropriate collection, sharing, or use of data from a child.
   - Significant findings from the compliance audit.
   - Work papers from the prior examination.

5. Determine the following through early discussions with management:

   - Management supervision of compliance with COPPA, including responsiveness to, and corrective measures resulting from, consumer complaint activity.
   - Changes in processes, including forms, contracts, software programs, etc., since the previous examination.
   - Significant changes in policies, personnel, or controls.
   - Internal or external factors that could affect compliance with COPPA.
   - Whether applicable provisions of state laws and regulations are monitored and included in the bank's audit.

6. Complete the "Quality of Risk Management" procedures.

7. Complete appropriate sections of the "Quantity of Risk" procedures. The procedures performed in the "Quantity of Risk" section should address areas of concern identified during the review of "Quality of Risk Management."

8. Complete the "Conclusion Procedures."

Quality of Risk Management

Conclusion: The quality of risk management is (strong, satisfactory, weak).

Policy

Conclusion: The board (has/has not) established appropriate policies to ensure compliance with the Children's Online Privacy Protect Act.

Objective: Determine whether the bank has appropriate formal/informal policies to ensure compliance with COPPA.

1. Determine whether the board has adopted, and management has implemented adequate policies and procedures to maintain compliance with COPPA. Where appropriate, they should address:

   - Significant requirements of the law and the regulation.
   - Responsibilities and accountabilities of key personnel.
   - Training program.
   - Process for responding to changes in the law and the regulation.
   - Role of audit and compliance review.

2. Determine whether the board or an appropriate committee periodically reviews and approves compliance policies.

Processes

Conclusion: Management (has/has not) established effective processes to ensure compliance with COPPA.

Objective: Determine the reliance that can be placed on the bank's processes to prevent violations of COPPA.

1. Determine whether the bank's system for communicating the requirements of, and any subsequent changes to, COPPA is adequate to ensure ongoing compliance.

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

- Organization chart to determine who is responsible for the institution's compliance with COPPA;
- Process flow charts 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 Web site or online service;
- List of data elements collected from a child and a description of how the data are used and protected;
- List of data elements collected from a child that are disclosed to third parties and any contracts or agreements governing the use of that information with those third parties;
- Internal checklists, worksheets, and other review documents.

3. Assess the procedures used to ensure compliance when new online products are developed and operational changes are made.

Personnel

Conclusion: Bank management and personnel (do/do not) possess the required technical skills and knowledge to ensure compliance with COPPA.

Objective: Determine whether bank management and personnel possess sufficient knowledge and technical skills to manage and perform duties related to COPPA.

1. Assess bank management and personnel's knowledge and technical skills regarding COPPA based on conclusions developed while performing these procedures. Also consider:
   - Employee roles and responsibilities.
   - Training and experience.
   - Violations cited.
2. Review the bank's training program (materials, agendas, rosters, frequency, evaluation forms, etc.) and discuss with management to

determine how frequently and how well employees are trained regarding compliance with COPPA.

Controls

Conclusion: Management (has/has not) established effective control systems to ensure compliance with COPPA.

Objective: Determine the reliance that can be placed on the bank's control systems to detect and correct violations of COPPA, including practices and procedures performed by audit and compliance review.

1. Review audit and compliance review material, including working papers and reports, to determine whether:

    - The procedures address the COPPA provisions applicable to the institution;
    - The audits and reviews performed were reasonable and accurate;
    - The frequency of the compliance review is satisfactory;
    - Effective corrective action occurred in response to previously identified deficiencies; and
    - Deficiencies, their causes, and the effective corrective actions are consistently reported to management or the members of the board of directors.

2. Review the following documents and discuss with management to determine whether management information systems are sufficient and whether adequate practices are in place to ensure that timely and appropriate corrective action is taken when weaknesses/violations are identified or when consumer complaints indicate significant deficiencies.

    - Audit/compliance review policies, procedures, and work papers.
    - Audit/compliance review reports and management responses.
    - Management reports.

Quantity of Risk Management

Conclusion: The quantity of risk is (low, moderate, high).

Perform only those procedures identified as areas of concern during the review of the "Quality of Risk Management."

Objective: Determine the bank's level of compliance with COPPA.

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

   - Data are collected, used and shared in accordance with the institution's Web site notice [16 CFR 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 [16 CFR 312.5(a)].

2. Through discussions with management and a review of policies and procedures, determine whether the 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].

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

4. Through testing or management's demonstration of the Web site or online service, verify that the financial institution does not condition 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 is reasonably necessary to participate in the activity [16 CFR 312.7].

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

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

- Complies with a parent's instructions concerning the collection, use, maintenance, or disclosure of his or her child's information. [16 CFR 312.6(a)(2) and 16 CFR 312.4(b)(2)(iv) and (vi)];

- Allows a parent to review any personal information collected from his or her child [16 CFR 312.6(a)(3)]; and

- Verifies that the person requesting information is a parent of the child [16 CFR 312.6 (a)(3)].

6. Complete the "COPPA Worksheet For Notices" by reviewing notices on the Web site or online service.

Conclusions

Objective: Prepare written conclusion summaries, discuss findings with the EIC, and communicate findings to management. If necessary, initiate corrective action when policies or internal controls are deficient or when violations of law or regulation are identified.

1. Summarize findings and violations from the preceding procedural steps to assess the bank's level of compliance with COPPA.

2. For those violations found to be significant or a pattern or practice, determine the root cause of violation(s) by identifying weaknesses in:

   - Internal controls.
   - Audit/independent compliance review.
   - Training.
   - Management oversight.

3. Determine whether a civil money penalty (CMP) or an enforcement action should be recommended (refer to the CMP matrix).

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

5. Form a conclusion about the reliability of the compliance management system for COPPA and provide conclusions to the examiner performing the Compliance Management System program.

6. Determine whether any items identified during this examination could materialize into supervisory concerns before the next on-site examination (considering whether the bank has plans to increase monitoring in the affected area, or anticipates changes in personnel, policy, outside auditors or consultants, or business strategy). If so, summarize your concerns and assess the potential risk to the bank.

7. Determine the impact on the aggregate quantity and direction of risk assessment for any concerns identified during the review. Examiners should refer to guidance provided under the OCC's large and community bank risk assessment programs.

   - Risk categories: compliance, transaction, and reputation risk.
   - Risk conclusions: high, moderate, or low.

- Risk direction: increasing, stable, or declining.

8. Provide, and discuss with, the EIC (and the supervisory office, if appropriate) conclusions, including:

   - A summary of violations and recommended CMPs/enforcement actions, if any.
   - Potential reimbursements.
   - Recommended corrective action.
   - The quantity of risk and quality of risk management.
   - Recommended matters requiring attention (MRA). MRA should cover practices that:
     – Deviate from sound fundamental principles and are likely to result in financial deterioration if not addressed.
     – Result in substantive noncompliance with laws.
   - MRA should discuss:
     – Causative factors contributing to the problem.
     – Consequences of inaction to the institution.
     – Management's commitment for corrective action.
     – The time frame and person(s) responsible for corrective action.

9. Discuss findings with management. Obtain commitment(s) for corrective action as needed. Include in the discussion:

   - The quality of risk management.
   - The quantity of risk (include a listing of all violations, as well as significant violations).
   - MRA(s).

10. As appropriate, prepare a brief comment for inclusion in the report of examination.

11. Prepare a memorandum summarizing work performed (e.g., sampling method used, internal control systems, scope of audit review, conclusions regarding audit, etc.) and update the work program with any information that will facilitate future examinations. Update the OCC database on all violations of law or regulation.

12. Organize and reference working papers in accordance with OCC guidance (PPM 5400-8).

Children's Online Privacy Protection Act Worksheet for Notices

Every "No" answer indicates a potential violation of the regulation or an internal control deficiency and must be fully explained in the work papers.

Web site Notice (16 CFR 312.4)	**Yes**	**No**
1. A Web site link is posted 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 Web site's information practices with regard to children, and is 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 [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 Web site [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 [16 CFR 312.4(b)(2)(iv)]: – 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; • 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 • That 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 – The notice states the procedures for doing so [16 CFR 312.4(b)(2)(vi)].		
4. The notice to a parent • States that the operator wishes to collect information from the child [16 CFR 312.4(c)(1)(i)(A)]. • Includes the information contained in the 16 CFR 312.4(b) Web site notice (see step 3 above) [16 CFR 312.4(c)(1)(i)]. • If 16 CFR 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 16 CFR 312.5(c)(3) and (4) apply.		

Request Letter Enclosure

1. COPPA policies and procedures.

2. COPPA training materials.

3. COPPA compliance reports, audit reports, procedures, and management responses. Note: If the bank participates in an FTC-approved, self-regulatory program, provide a copy of the program and audit reports.

4. Complaints regarding the collection, sharing, or use of data from a child.

5. Copies of Web site notices since the last examination.

6. A list of data elements collected from a child and a description of how the data are used and protected.

7. A list of data elements collected from a child that are disclosed to third parties and any contracts or agreements governing the use of that information with those third parties.

8. A list of parental requests for personal information provided by their children.

9. A description of how parental permission is obtained and the method of verifying that the person providing consent is the child's parent.

Laws

15 USC 6501 et seq., Children's Online Privacy Protection Act

Regulations

16 CFR 312, Children's Online Privacy Protection Rule

OCC Issuances

Bulletin 2001-8, "Guidelines Establishing Standards for Safeguarding Customer Information," dated 02/05/01.

Bulletin 2001-26, "Privacy of Consumer Financial Information; 12 CFR 40," dated 05/25/01.

Bulletin 2001-31, Weblinking," dated 07/03/01.

Bulletin 2001-35, "Examination Procedures to Evaluate Compliance with Guidelines to Safeguard Customer Information," dated 07/18/01.

Advisory Letter 2001-08, "Authentication in an Electronic Banking Environment," dated 07/30/01.

CHILDREN'S ONLINE PRIVACY PROTECTION ACT

Children's Online Privacy Protection Act

Table of Contents

Children's Online Privacy Protection Act

Introduction

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 that is collected from children through Web sites 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 Web site(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.

Financial institutions that do not currently operate a Web site or online service directed to children, or do not have actual knowledge that they are collecting or maintaining personal information from a child online, are not subject to COPPA and will not be subject to COPPA examinations by the Office of the Comptroller of the Currency (OCC). However, financial institutions are urged to review their Web sites and their online information collection practices to ensure that they do not inadvertently trigger the provisions of this Act.

Definitions

"Child", "Children": (an) individual(s) under the age of 13.

"Personal information": 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 Web site 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 to the parent and on the Web site 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 and have deleted the personal information collected from his or 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).

Notice on the Web Site

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

An operator of a Web site or online service directed to children must post a link to a notice of its information practices with regard to children on its home page and at each area on the site or service where it collects personal information from any child. 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.

These links must be placed in a clear and prominent location on the home page of the Web site 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 that requires visitors to scroll down the 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 child through the Web site or online service;

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

- The way the operator uses, or may use, the personal information;

- A statement of 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 there is a prohibition against requiring, 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 has a right to 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 child can be made. 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's wishes to collect personal information from the parent's child;

- The requirement of the parent's consent for the collection, use, and disclosure of the information; and

- The way(s) the parent can provide consent.

Internal Uses [16 CFR 312.5(b)]

Financial institutions that use the personal information solely for internal purposes 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.

Disclosure to Others [16 CFR 312.5(b)]

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 requires a more reliable method of consent. The method used to obtain verifiable parental consent must be reasonably calculated, in light of available technology, to ensure that the person providing the consent is the child's parent. Methods that satisfy this requirement include:

- Obtaining a signed consent form from a parent via postal mail or facsimile;

- Accepting and verifying a parent's credit card number;

- Taking a parent's call, through a toll-free telephone number staffed by trained personnel;

- Receiving a parent's e-mail, accompanied by a digital signature; and

- Receiving an e-mail from a parent that is accompanied by a personal identification number (PIN) or password obtained through one of the methods mentioned above.

Disclosures to Third Parties [16 CFR 312.5(a)]

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 [16 CFR 312.5(a)]

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 [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 period 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 to, on a one-time basis, 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 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 Web site or online service is required to provide to a parent a means by which he or she can obtain any personal information collected from his or her child by that operator. 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. These methods might include requiring a parent to use a credit card in connection with a transaction; having a parent call a toll-free number staffed by trained personnel; using a digital certificate that uses public key technology; or using e-mail accompanied by a PIN or password.

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 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 any child.

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 Web site or online service that complies with FTC-approved, self-regulatory guidelines will receive a "safe harbor" from the requirements of COPPA and the regulation.

To be approved by the FTC, self-regulatory guidelines must include a requirement that operators subject to the guidelines implement substantially similar requirements that provide the same or greater protections for a child as the FTC regulation (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.

General Procedures

Objective: Determine the scope of the Children's Online Privacy Protection Act (COPPA) examination.

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

   - Is directed to children; or
   - Knowingly collects or maintains personal information from children.

   If the institution does not currently operate a Web site directed to children or knowingly collect information about them, the institution is not subject to COPPA, and no further examination for COPPA is necessary.

2. If the institution is subject to COPPA, determine whether it is participating in an FTC-approved, self-regulatory program (see 16 CFR 312.10). If it is, obtain a copy of the program and supporting documentation, such as reviews or audits, that demonstrate the institution's compliance with the program. If, under the self-regulatory program, an independent assessment found the institution in compliance with COPPA, or no assessment has yet been made, no further examination for COPPA is necessary. If, however, the independent assessment found the institution not in compliance with COPPA and the institution has not taken appropriate corrective action, continue with the procedures below.

3. If the institution is subject to COPPA and is not participating in an FTC-approved, self-regulatory program, continue with the procedures below.

4. From the examiner assigned the Compliance Management System program, obtain and review the following information to identify any previous or emerging problems that require follow-up:

   - Historical examination findings.
   - Complaint information from the bank and the OCC's Customer Assistance Group (CAG), and any CAG analytical reports, regarding the inappropriate collection, sharing, or use of data from a child.
   - Significant findings from the compliance audit.
   - Work papers from the prior examination.

5. Determine the following through early discussions with management:

   - Management supervision of compliance with COPPA, including responsiveness to, and corrective measures resulting from, consumer complaint activity.
   - Changes in processes, including forms, contracts, software programs, etc., since the previous examination.
   - Significant changes in policies, personnel, or controls.
   - Internal or external factors that could affect compliance with COPPA.
   - Whether applicable provisions of state laws and regulations are monitored and included in the bank's audit.

6. Complete the "Quality of Risk Management" procedures.

7. Complete appropriate sections of the "Quantity of Risk" procedures. The procedures performed in the "Quantity of Risk" section should address areas of concern identified during the review of "Quality of Risk Management."

8. Complete the "Conclusion Procedures."

Quality of Risk Management

Conclusion: The quality of risk management is (strong, satisfactory, weak).

Policy

Conclusion: The board (has/has not) established appropriate policies to ensure compliance with the Children's Online Privacy Protect Act.

Objective: Determine whether the bank has appropriate formal/informal policies to ensure compliance with COPPA.

1. Determine whether the board has adopted, and management has implemented adequate policies and procedures to maintain compliance with COPPA. Where appropriate, they should address:

   - Significant requirements of the law and the regulation.
   - Responsibilities and accountabilities of key personnel.
   - Training program.
   - Process for responding to changes in the law and the regulation.
   - Role of audit and compliance review.

2. Determine whether the board or an appropriate committee periodically reviews and approves compliance policies.

Processes

Conclusion: Management (has/has not) established effective processes to ensure compliance with COPPA.

Objective: Determine the reliance that can be placed on the bank's processes to prevent violations of COPPA.

1. Determine whether the bank's system for communicating the requirements of, and any subsequent changes to, COPPA is adequate to ensure ongoing compliance.

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

- Organization chart to determine who is responsible for the institution's compliance with COPPA;
- Process flow charts 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 Web site or online service;
- List of data elements collected from a child and a description of how the data are used and protected;
- List of data elements collected from a child that are disclosed to third parties and any contracts or agreements governing the use of that information with those third parties;
- Internal checklists, worksheets, and other review documents.

3. Assess the procedures used to ensure compliance when new online products are developed and operational changes are made.

Personnel

Conclusion: Bank management and personnel (do/do not) possess the required technical skills and knowledge to ensure compliance with COPPA.

Objective: Determine whether bank management and personnel possess sufficient knowledge and technical skills to manage and perform duties related to COPPA.

1. Assess bank management and personnel's knowledge and technical skills regarding COPPA based on conclusions developed while performing these procedures. Also consider:
   - Employee roles and responsibilities.
   - Training and experience.
   - Violations cited.
2. Review the bank's training program (materials, agendas, rosters, frequency, evaluation forms, etc.) and discuss with management to

determine how frequently and how well employees are trained regarding compliance with COPPA.

Controls

Conclusion: Management (has/has not) established effective control systems to ensure compliance with COPPA.

Objective: Determine the reliance that can be placed on the bank's control systems to detect and correct violations of COPPA, including practices and procedures performed by audit and compliance review.

1. Review audit and compliance review material, including working papers and reports, to determine whether:

    - The procedures address the COPPA provisions applicable to the institution;
    - The audits and reviews performed were reasonable and accurate;
    - The frequency of the compliance review is satisfactory;
    - Effective corrective action occurred in response to previously identified deficiencies; and
    - Deficiencies, their causes, and the effective corrective actions are consistently reported to management or the members of the board of directors.

2. Review the following documents and discuss with management to determine whether management information systems are sufficient and whether adequate practices are in place to ensure that timely and appropriate corrective action is taken when weaknesses/violations are identified or when consumer complaints indicate significant deficiencies.

    - Audit/compliance review policies, procedures, and work papers.
    - Audit/compliance review reports and management responses.
    - Management reports.

Quantity of Risk Management

Conclusion: The quantity of risk is (low, moderate, high).

Perform only those procedures identified as areas of concern during the review of the "Quality of Risk Management."

Objective: Determine the bank's level of compliance with COPPA.

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

   - Data are collected, used and shared in accordance with the institution's Web site notice [16 CFR 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 [16 CFR 312.5(a)].

2. Through discussions with management and a review of policies and procedures, determine whether the 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].

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

4. Through testing or management's demonstration of the Web site or online service, verify that the financial institution does not condition 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 is reasonably necessary to participate in the activity [16 CFR 312.7].

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

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

- Complies with a parent's instructions concerning the collection, use, maintenance, or disclosure of his or her child's information. [16 CFR 312.6(a)(2) and 16 CFR 312.4(b)(2)(iv) and (vi)];

- Allows a parent to review any personal information collected from his or her child [16 CFR 312.6(a)(3)]; and

- Verifies that the person requesting information is a parent of the child [16 CFR 312.6 (a)(3)].

6. Complete the "COPPA Worksheet For Notices" by reviewing notices on the Web site or online service.

Conclusions

Objective: Prepare written conclusion summaries, discuss findings with the EIC, and communicate findings to management. If necessary, initiate corrective action when policies or internal controls are deficient or when violations of law or regulation are identified.

1. Summarize findings and violations from the preceding procedural steps to assess the bank's level of compliance with COPPA.

2. For those violations found to be significant or a pattern or practice, determine the root cause of violation(s) by identifying weaknesses in:

   - Internal controls.
   - Audit/independent compliance review.
   - Training.
   - Management oversight.

3. Determine whether a civil money penalty (CMP) or an enforcement action should be recommended (refer to the CMP matrix).

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

5. Form a conclusion about the reliability of the compliance management system for COPPA and provide conclusions to the examiner performing the Compliance Management System program.

6. Determine whether any items identified during this examination could materialize into supervisory concerns before the next on-site examination (considering whether the bank has plans to increase monitoring in the affected area, or anticipates changes in personnel, policy, outside auditors or consultants, or business strategy). If so, summarize your concerns and assess the potential risk to the bank.

7. Determine the impact on the aggregate quantity and direction of risk assessment for any concerns identified during the review. Examiners should refer to guidance provided under the OCC's large and community bank risk assessment programs.

   - Risk categories: compliance, transaction, and reputation risk.
   - Risk conclusions: high, moderate, or low.

- Risk direction: increasing, stable, or declining.

8. Provide, and discuss with, the EIC (and the supervisory office, if appropriate) conclusions, including:

   - A summary of violations and recommended CMPs/enforcement actions, if any.
   - Potential reimbursements.
   - Recommended corrective action.
   - The quantity of risk and quality of risk management.
   - Recommended matters requiring attention (MRA). MRA should cover practices that:
     – Deviate from sound fundamental principles and are likely to result in financial deterioration if not addressed.
     – Result in substantive noncompliance with laws.
   - MRA should discuss:
     – Causative factors contributing to the problem.
     – Consequences of inaction to the institution.
     – Management's commitment for corrective action.
     – The time frame and person(s) responsible for corrective action.

9. Discuss findings with management. Obtain commitment(s) for corrective action as needed. Include in the discussion:

   - The quality of risk management.
   - The quantity of risk (include a listing of all violations, as well as significant violations).
   - MRA(s).

10. As appropriate, prepare a brief comment for inclusion in the report of examination.

11. Prepare a memorandum summarizing work performed (e.g., sampling method used, internal control systems, scope of audit review, conclusions regarding audit, etc.) and update the work program with any information that will facilitate future examinations. Update the OCC database on all violations of law or regulation.

12. Organize and reference working papers in accordance with OCC guidance (PPM 5400-8).

Children's Online Privacy Protection Act Worksheet for Notices

Every "No" answer indicates a potential violation of the regulation or an internal control deficiency and must be fully explained in the work papers.

Web site Notice (16 CFR 312.4)	**Yes**	**No**
1. A Web site link is posted 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 Web site's information practices with regard to children, and is 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 [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 Web site [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 [16 CFR 312.4(b)(2)(iv)]: – 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; • 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 • That 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 – The notice states the procedures for doing so [16 CFR 312.4(b)(2)(vi)].		
4. The notice to a parent • States that the operator wishes to collect information from the child [16 CFR 312.4(c)(1)(i)(A)]. • Includes the information contained in the 16 CFR 312.4(b) Web site notice (see step 3 above) [16 CFR 312.4(c)(1)(i)]. • If 16 CFR 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 16 CFR 312.5(c)(3) and (4) apply.		

Request Letter Enclosure

1. COPPA policies and procedures.

2. COPPA training materials.

3. COPPA compliance reports, audit reports, procedures, and management responses. Note: If the bank participates in an FTC-approved, self-regulatory program, provide a copy of the program and audit reports.

4. Complaints regarding the collection, sharing, or use of data from a child.

5. Copies of Web site notices since the last examination.

6. A list of data elements collected from a child and a description of how the data are used and protected.

7. A list of data elements collected from a child that are disclosed to third parties and any contracts or agreements governing the use of that information with those third parties.

8. A list of parental requests for personal information provided by their children.

9. A description of how parental permission is obtained and the method of verifying that the person providing consent is the child's parent.

Laws

15 USC 6501 et seq., Children's Online Privacy Protection Act

Regulations

16 CFR 312, Children's Online Privacy Protection Rule

OCC Issuances

Bulletin 2001-8, "Guidelines Establishing Standards for Safeguarding Customer Information," dated 02/05/01.

Bulletin 2001-26, "Privacy of Consumer Financial Information; 12 CFR 40," dated 05/25/01.

Bulletin 2001-31, Weblinking," dated 07/03/01.

Bulletin 2001-35, "Examination Procedures to Evaluate Compliance with Guidelines to Safeguard Customer Information," dated 07/18/01.

Advisory Letter 2001-08, "Authentication in an Electronic Banking Environment," dated 07/30/01.

CHILDREN'S ONLINE PRIVACY PROTECTION ACT

Comptroller of the Currency
Administrator of National Banks
US Department of the Treasury

OCC 2002-31

Subject: Children's Online Privacy Protection Act (COPPA)
Date: July 16, 2002

To: Chief Executive Officers and Compliance Officers of All National Banks, Department and Division Heads, and All Examining Personnel

Description: Examination Procedures

Attached are examination procedures for the Children's Online Privacy Protection Act (COPPA) that are effective immediately. COPPA addresses the collection, use, or disclosure of personal information that is collected from children through Web sites or other online services. Financial institutions that do not currently operate a Web site or online service directed to children or that do not have actual knowledge that they are collecting or maintaining personal information from a child online are not subject to COPPA and will not be subject to COPPA examinations by the OCC. However, financial institutions are urged to review their Web sites and their online information collection practices to ensure that they do not inadvertently trigger the provisions of this act.

The Federal Trade Commission issued a regulation, 16 CFR 312, implementing COPPA. It became effective on April 21, 2000.

For more information, contact your supervisory office or the Compliance Department at (202) 874-4428.

David G. Hammaker
Deputy Comptroller for Compliance

Related Links

- COPPA Examination Procedures

CHILDREN'S ONLINE PRIVACY PROTECTION ACT

Children's Online Privacy Protection Act

Table of Contents

Children's Online Privacy Protection Act

Introduction

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 that is collected from children through Web sites 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 Web site(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.

Financial institutions that do not currently operate a Web site or online service directed to children, or do not have actual knowledge that they are collecting or maintaining personal information from a child online, are not subject to COPPA and will not be subject to COPPA examinations by the Office of the Comptroller of the Currency (OCC). However, financial institutions are urged to review their Web sites and their online information collection practices to ensure that they do not inadvertently trigger the provisions of this Act.

Definitions

"Child", "Children": (an) individual(s) under the age of 13.

"Personal information": 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 Web site 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 to the parent and on the Web site 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 and have deleted the personal information collected from his or 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).

Notice on the Web Site

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

An operator of a Web site or online service directed to children must post a link to a notice of its information practices with regard to children on its home page and at each area on the site or service where it collects personal information from any child. 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.

These links must be placed in a clear and prominent location on the home page of the Web site 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 that requires visitors to scroll down the 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 child through the Web site or online service;

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

- The way the operator uses, or may use, the personal information;

- A statement of 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 there is a prohibition against requiring, 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 has a right to 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 child can be made. 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's wishes to collect personal information from the parent's child;

- The requirement of the parent's consent for the collection, use, and disclosure of the information; and

- The way(s) the parent can provide consent.

Internal Uses [16 CFR 312.5(b)]

Financial institutions that use the personal information solely for internal purposes 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.

Disclosure to Others [16 CFR 312.5(b)]

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 requires a more reliable method of consent. The method used to obtain verifiable parental consent must be reasonably calculated, in light of available technology, to ensure that the person providing the consent is the child's parent. Methods that satisfy this requirement include:

- Obtaining a signed consent form from a parent via postal mail or facsimile;

- Accepting and verifying a parent's credit card number;

- Taking a parent's call, through a toll-free telephone number staffed by trained personnel;

- Receiving a parent's e-mail, accompanied by a digital signature; and

- Receiving an e-mail from a parent that is accompanied by a personal identification number (PIN) or password obtained through one of the methods mentioned above.

Disclosures to Third Parties [16 CFR 312.5(a)]

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 [16 CFR 312.5(a)]

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 [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 period 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 to, on a one-time basis, 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 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 Web site or online service is required to provide to a parent a means by which he or she can obtain any personal information collected from his or her child by that operator. 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. These methods might include requiring a parent to use a credit card in connection with a transaction; having a parent call a toll-free number staffed by trained personnel; using a digital certificate that uses public key technology; or using e-mail accompanied by a PIN or password.

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 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 any child.

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 Web site or online service that complies with FTC-approved, self-regulatory guidelines will receive a "safe harbor" from the requirements of COPPA and the regulation.

To be approved by the FTC, self-regulatory guidelines must include a requirement that operators subject to the guidelines implement substantially similar requirements that provide the same or greater protections for a child as the FTC regulation (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.

General Procedures

Objective: Determine the scope of the Children's Online Privacy Protection Act (COPPA) examination.

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

   - Is directed to children; or
   - Knowingly collects or maintains personal information from children.

   If the institution does not currently operate a Web site directed to children or knowingly collect information about them, the institution is not subject to COPPA, and no further examination for COPPA is necessary.

2. If the institution is subject to COPPA, determine whether it is participating in an FTC-approved, self-regulatory program (see 16 CFR 312.10). If it is, obtain a copy of the program and supporting documentation, such as reviews or audits, that demonstrate the institution's compliance with the program. If, under the self-regulatory program, an independent assessment found the institution in compliance with COPPA, or no assessment has yet been made, no further examination for COPPA is necessary. If, however, the independent assessment found the institution not in compliance with COPPA and the institution has not taken appropriate corrective action, continue with the procedures below.

3. If the institution is subject to COPPA and is not participating in an FTC-approved, self-regulatory program, continue with the procedures below.

4. From the examiner assigned the Compliance Management System program, obtain and review the following information to identify any previous or emerging problems that require follow-up:

   - Historical examination findings.
   - Complaint information from the bank and the OCC's Customer Assistance Group (CAG), and any CAG analytical reports, regarding the inappropriate collection, sharing, or use of data from a child.
   - Significant findings from the compliance audit.
   - Work papers from the prior examination.

5. Determine the following through early discussions with management:

   - Management supervision of compliance with COPPA, including responsiveness to, and corrective measures resulting from, consumer complaint activity.
   - Changes in processes, including forms, contracts, software programs, etc., since the previous examination.
   - Significant changes in policies, personnel, or controls.
   - Internal or external factors that could affect compliance with COPPA.
   - Whether applicable provisions of state laws and regulations are monitored and included in the bank's audit.

6. Complete the "Quality of Risk Management" procedures.

7. Complete appropriate sections of the "Quantity of Risk" procedures. The procedures performed in the "Quantity of Risk" section should address areas of concern identified during the review of "Quality of Risk Management."

8. Complete the "Conclusion Procedures."

Quality of Risk Management

Conclusion: The quality of risk management is (strong, satisfactory, weak).

Policy

Conclusion: The board (has/has not) established appropriate policies to ensure compliance with the Children's Online Privacy Protect Act.

Objective: Determine whether the bank has appropriate formal/informal policies to ensure compliance with COPPA.

1. Determine whether the board has adopted, and management has implemented adequate policies and procedures to maintain compliance with COPPA. Where appropriate, they should address:

   - Significant requirements of the law and the regulation.
   - Responsibilities and accountabilities of key personnel.
   - Training program.
   - Process for responding to changes in the law and the regulation.
   - Role of audit and compliance review.

2. Determine whether the board or an appropriate committee periodically reviews and approves compliance policies.

Processes

Conclusion: Management (has/has not) established effective processes to ensure compliance with COPPA.

Objective: Determine the reliance that can be placed on the bank's processes to prevent violations of COPPA.

1. Determine whether the bank's system for communicating the requirements of, and any subsequent changes to, COPPA is adequate to ensure ongoing compliance.

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

- Organization chart to determine who is responsible for the institution's compliance with COPPA;
- Process flow charts 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 Web site or online service;
- List of data elements collected from a child and a description of how the data are used and protected;
- List of data elements collected from a child that are disclosed to third parties and any contracts or agreements governing the use of that information with those third parties;
- Internal checklists, worksheets, and other review documents.

3. Assess the procedures used to ensure compliance when new online products are developed and operational changes are made.

Personnel

Conclusion: Bank management and personnel (do/do not) possess the required technical skills and knowledge to ensure compliance with COPPA.

Objective: Determine whether bank management and personnel possess sufficient knowledge and technical skills to manage and perform duties related to COPPA.

1. Assess bank management and personnel's knowledge and technical skills regarding COPPA based on conclusions developed while performing these procedures. Also consider:
   - Employee roles and responsibilities.
   - Training and experience.
   - Violations cited.
2. Review the bank's training program (materials, agendas, rosters, frequency, evaluation forms, etc.) and discuss with management to

determine how frequently and how well employees are trained regarding compliance with COPPA.

Controls

Conclusion: Management (has/has not) established effective control systems to ensure compliance with COPPA.

Objective: Determine the reliance that can be placed on the bank's control systems to detect and correct violations of COPPA, including practices and procedures performed by audit and compliance review.

1. Review audit and compliance review material, including working papers and reports, to determine whether:

   - The procedures address the COPPA provisions applicable to the institution;
   - The audits and reviews performed were reasonable and accurate;
   - The frequency of the compliance review is satisfactory;
   - Effective corrective action occurred in response to previously identified deficiencies; and
   - Deficiencies, their causes, and the effective corrective actions are consistently reported to management or the members of the board of directors.

2. Review the following documents and discuss with management to determine whether management information systems are sufficient and whether adequate practices are in place to ensure that timely and appropriate corrective action is taken when weaknesses/violations are identified or when consumer complaints indicate significant deficiencies.

   - Audit/compliance review policies, procedures, and work papers.
   - Audit/compliance review reports and management responses.
   - Management reports.

Quantity of Risk Management

Conclusion: The quantity of risk is (low, moderate, high).

Perform only those procedures identified as areas of concern during the review of the "Quality of Risk Management."

Objective: Determine the bank's level of compliance with COPPA.

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

   - Data are collected, used and shared in accordance with the institution's Web site notice [16 CFR 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 [16 CFR 312.5(a)].

2. Through discussions with management and a review of policies and procedures, determine whether the 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].

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

4. Through testing or management's demonstration of the Web site or online service, verify that the financial institution does not condition 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 is reasonably necessary to participate in the activity [16 CFR 312.7].

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

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

- Complies with a parent's instructions concerning the collection, use, maintenance, or disclosure of his or her child's information. [16 CFR 312.6(a)(2) and 16 CFR 312.4(b)(2)(iv) and (vi)];

- Allows a parent to review any personal information collected from his or her child [16 CFR 312.6(a)(3)]; and

- Verifies that the person requesting information is a parent of the child [16 CFR 312.6 (a)(3)].

6. Complete the "COPPA Worksheet For Notices" by reviewing notices on the Web site or online service.

Conclusions

Objective: Prepare written conclusion summaries, discuss findings with the EIC, and communicate findings to management. If necessary, initiate corrective action when policies or internal controls are deficient or when violations of law or regulation are identified.

1. Summarize findings and violations from the preceding procedural steps to assess the bank's level of compliance with COPPA.

2. For those violations found to be significant or a pattern or practice, determine the root cause of violation(s) by identifying weaknesses in:

   - Internal controls.
   - Audit/independent compliance review.
   - Training.
   - Management oversight.

3. Determine whether a civil money penalty (CMP) or an enforcement action should be recommended (refer to the CMP matrix).

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

5. Form a conclusion about the reliability of the compliance management system for COPPA and provide conclusions to the examiner performing the Compliance Management System program.

6. Determine whether any items identified during this examination could materialize into supervisory concerns before the next on-site examination (considering whether the bank has plans to increase monitoring in the affected area, or anticipates changes in personnel, policy, outside auditors or consultants, or business strategy). If so, summarize your concerns and assess the potential risk to the bank.

7. Determine the impact on the aggregate quantity and direction of risk assessment for any concerns identified during the review. Examiners should refer to guidance provided under the OCC's large and community bank risk assessment programs.

   - Risk categories: compliance, transaction, and reputation risk.
   - Risk conclusions: high, moderate, or low.

- Risk direction: increasing, stable, or declining.

8. Provide, and discuss with, the EIC (and the supervisory office, if appropriate) conclusions, including:

   - A summary of violations and recommended CMPs/enforcement actions, if any.
   - Potential reimbursements.
   - Recommended corrective action.
   - The quantity of risk and quality of risk management.
   - Recommended matters requiring attention (MRA). MRA should cover practices that:
     – Deviate from sound fundamental principles and are likely to result in financial deterioration if not addressed.
     – Result in substantive noncompliance with laws.
   - MRA should discuss:
     – Causative factors contributing to the problem.
     – Consequences of inaction to the institution.
     – Management's commitment for corrective action.
     – The time frame and person(s) responsible for corrective action.

9. Discuss findings with management. Obtain commitment(s) for corrective action as needed. Include in the discussion:

   - The quality of risk management.
   - The quantity of risk (include a listing of all violations, as well as significant violations).
   - MRA(s).

10. As appropriate, prepare a brief comment for inclusion in the report of examination.

11. Prepare a memorandum summarizing work performed (e.g., sampling method used, internal control systems, scope of audit review, conclusions regarding audit, etc.) and update the work program with any information that will facilitate future examinations. Update the OCC database on all violations of law or regulation.

12. Organize and reference working papers in accordance with OCC guidance (PPM 5400-8).

Children's Online Privacy Protection Act Worksheet for Notices

Every "No" answer indicates a potential violation of the regulation or an internal control deficiency and must be fully explained in the work papers.

Web site Notice (16 CFR 312.4)	**Yes**	**No**
1. A Web site link is posted 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 Web site's information practices with regard to children, and is 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 [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 Web site [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 [16 CFR 312.4(b)(2)(iv)]: – 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; • 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 • That 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 – The notice states the procedures for doing so [16 CFR 312.4(b)(2)(vi)].		
4. The notice to a parent • States that the operator wishes to collect information from the child [16 CFR 312.4(c)(1)(i)(A)]. • Includes the information contained in the 16 CFR 312.4(b) Web site notice (see step 3 above) [16 CFR 312.4(c)(1)(i)]. • If 16 CFR 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 16 CFR 312.5(c)(3) and (4) apply.		

Children's Online Privacy Protection Act

Appendix B

Request Letter Enclosure

1. COPPA policies and procedures.

2. COPPA training materials.

3. COPPA compliance reports, audit reports, procedures, and management responses. Note: If the bank participates in an FTC-approved, self-regulatory program, provide a copy of the program and audit reports.

4. Complaints regarding the collection, sharing, or use of data from a child.

5. Copies of Web site notices since the last examination.

6. A list of data elements collected from a child and a description of how the data are used and protected.

7. A list of data elements collected from a child that are disclosed to third parties and any contracts or agreements governing the use of that information with those third parties.

8. A list of parental requests for personal information provided by their children.

9. A description of how parental permission is obtained and the method of verifying that the person providing consent is the child's parent.

Laws

15 USC 6501 et seq., Children's Online Privacy Protection Act

Regulations

16 CFR 312, Children's Online Privacy Protection Rule

OCC Issuances

Bulletin 2001-8, "Guidelines Establishing Standards for Safeguarding Customer Information," dated 02/05/01.

Bulletin 2001-26, "Privacy of Consumer Financial Information; 12 CFR 40," dated 05/25/01.

Bulletin 2001-31, Weblinking," dated 07/03/01.

Bulletin 2001-35, "Examination Procedures to Evaluate Compliance with Guidelines to Safeguard Customer Information," dated 07/18/01.

Advisory Letter 2001-08, "Authentication in an Electronic Banking Environment," dated 07/30/01.

CHILDREN'S ONLINE PRIVACY PROTECTION ACT

Children's Online Privacy Protection Act

Table of Contents

Children's Online Privacy Protection Act

Introduction

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 that is collected from children through Web sites 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 Web site(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.

Financial institutions that do not currently operate a Web site or online service directed to children, or do not have actual knowledge that they are collecting or maintaining personal information from a child online, are not subject to COPPA and will not be subject to COPPA examinations by the Office of the Comptroller of the Currency (OCC). However, financial institutions are urged to review their Web sites and their online information collection practices to ensure that they do not inadvertently trigger the provisions of this Act.

Definitions

"Child", "Children": (an) individual(s) under the age of 13.

"Personal information": 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 Web site 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 to the parent and on the Web site 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 and have deleted the personal information collected from his or 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).

Notice on the Web Site

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

An operator of a Web site or online service directed to children must post a link to a notice of its information practices with regard to children on its home page and at each area on the site or service where it collects personal information from any child. 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.

These links must be placed in a clear and prominent location on the home page of the Web site 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 that requires visitors to scroll down the 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 child through the Web site or online service;

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

- The way the operator uses, or may use, the personal information;

- A statement of 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 there is a prohibition against requiring, 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 has a right to 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 child can be made. 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's wishes to collect personal information from the parent's child;

- The requirement of the parent's consent for the collection, use, and disclosure of the information; and

- The way(s) the parent can provide consent.

Internal Uses [16 CFR 312.5(b)]

Financial institutions that use the personal information solely for internal purposes 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.

Disclosure to Others [16 CFR 312.5(b)]

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 requires a more reliable method of consent. The method used to obtain verifiable parental consent must be reasonably calculated, in light of available technology, to ensure that the person providing the consent is the child's parent. Methods that satisfy this requirement include:

- Obtaining a signed consent form from a parent via postal mail or facsimile;

- Accepting and verifying a parent's credit card number;

- Taking a parent's call, through a toll-free telephone number staffed by trained personnel;

- Receiving a parent's e-mail, accompanied by a digital signature; and

- Receiving an e-mail from a parent that is accompanied by a personal identification number (PIN) or password obtained through one of the methods mentioned above.

Disclosures to Third Parties [16 CFR 312.5(a)]

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 [16 CFR 312.5(a)]

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 [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 period 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 to, on a one-time basis, 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 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 Web site or online service is required to provide to a parent a means by which he or she can obtain any personal information collected from his or her child by that operator. 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. These methods might include requiring a parent to use a credit card in connection with a transaction; having a parent call a toll-free number staffed by trained personnel; using a digital certificate that uses public key technology; or using e-mail accompanied by a PIN or password.

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 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 any child.

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 Web site or online service that complies with FTC-approved, self-regulatory guidelines will receive a "safe harbor" from the requirements of COPPA and the regulation.

To be approved by the FTC, self-regulatory guidelines must include a requirement that operators subject to the guidelines implement substantially similar requirements that provide the same or greater protections for a child as the FTC regulation (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.

General Procedures

Objective: Determine the scope of the Children's Online Privacy Protection Act (COPPA) examination.

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

   - Is directed to children; or
   - Knowingly collects or maintains personal information from children.

   If the institution does not currently operate a Web site directed to children or knowingly collect information about them, the institution is not subject to COPPA, and no further examination for COPPA is necessary.

2. If the institution is subject to COPPA, determine whether it is participating in an FTC-approved, self-regulatory program (see 16 CFR 312.10). If it is, obtain a copy of the program and supporting documentation, such as reviews or audits, that demonstrate the institution's compliance with the program. If, under the self-regulatory program, an independent assessment found the institution in compliance with COPPA, or no assessment has yet been made, no further examination for COPPA is necessary. If, however, the independent assessment found the institution not in compliance with COPPA and the institution has not taken appropriate corrective action, continue with the procedures below.

3. If the institution is subject to COPPA and is not participating in an FTC-approved, self-regulatory program, continue with the procedures below.

4. From the examiner assigned the Compliance Management System program, obtain and review the following information to identify any previous or emerging problems that require follow-up:

   - Historical examination findings.
   - Complaint information from the bank and the OCC's Customer Assistance Group (CAG), and any CAG analytical reports, regarding the inappropriate collection, sharing, or use of data from a child.
   - Significant findings from the compliance audit.
   - Work papers from the prior examination.

5. Determine the following through early discussions with management:

   - Management supervision of compliance with COPPA, including responsiveness to, and corrective measures resulting from, consumer complaint activity.
   - Changes in processes, including forms, contracts, software programs, etc., since the previous examination.
   - Significant changes in policies, personnel, or controls.
   - Internal or external factors that could affect compliance with COPPA.
   - Whether applicable provisions of state laws and regulations are monitored and included in the bank's audit.

6. Complete the "Quality of Risk Management" procedures.

7. Complete appropriate sections of the "Quantity of Risk" procedures. The procedures performed in the "Quantity of Risk" section should address areas of concern identified during the review of "Quality of Risk Management."

8. Complete the "Conclusion Procedures."

Quality of Risk Management

Conclusion: The quality of risk management is (strong, satisfactory, weak).

Policy

Conclusion: The board (has/has not) established appropriate policies to ensure compliance with the Children's Online Privacy Protect Act.

Objective: Determine whether the bank has appropriate formal/informal policies to ensure compliance with COPPA.

1. Determine whether the board has adopted, and management has implemented adequate policies and procedures to maintain compliance with COPPA. Where appropriate, they should address:

   - Significant requirements of the law and the regulation.
   - Responsibilities and accountabilities of key personnel.
   - Training program.
   - Process for responding to changes in the law and the regulation.
   - Role of audit and compliance review.

2. Determine whether the board or an appropriate committee periodically reviews and approves compliance policies.

Processes

Conclusion: Management (has/has not) established effective processes to ensure compliance with COPPA.

Objective: Determine the reliance that can be placed on the bank's processes to prevent violations of COPPA.

1. Determine whether the bank's system for communicating the requirements of, and any subsequent changes to, COPPA is adequate to ensure ongoing compliance.

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

- Organization chart to determine who is responsible for the institution's compliance with COPPA;
- Process flow charts 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 Web site or online service;
- List of data elements collected from a child and a description of how the data are used and protected;
- List of data elements collected from a child that are disclosed to third parties and any contracts or agreements governing the use of that information with those third parties;
- Internal checklists, worksheets, and other review documents.

3. Assess the procedures used to ensure compliance when new online products are developed and operational changes are made.

Personnel

Conclusion: Bank management and personnel (do/do not) possess the required technical skills and knowledge to ensure compliance with COPPA.

Objective: Determine whether bank management and personnel possess sufficient knowledge and technical skills to manage and perform duties related to COPPA.

1. Assess bank management and personnel's knowledge and technical skills regarding COPPA based on conclusions developed while performing these procedures. Also consider:
   - Employee roles and responsibilities.
   - Training and experience.
   - Violations cited.
2. Review the bank's training program (materials, agendas, rosters, frequency, evaluation forms, etc.) and discuss with management to

determine how frequently and how well employees are trained regarding compliance with COPPA.

Controls

Conclusion: Management (has/has not) established effective control systems to ensure compliance with COPPA.

Objective: Determine the reliance that can be placed on the bank's control systems to detect and correct violations of COPPA, including practices and procedures performed by audit and compliance review.

1. Review audit and compliance review material, including working papers and reports, to determine whether:

   - The procedures address the COPPA provisions applicable to the institution;
   - The audits and reviews performed were reasonable and accurate;
   - The frequency of the compliance review is satisfactory;
   - Effective corrective action occurred in response to previously identified deficiencies; and
   - Deficiencies, their causes, and the effective corrective actions are consistently reported to management or the members of the board of directors.

2. Review the following documents and discuss with management to determine whether management information systems are sufficient and whether adequate practices are in place to ensure that timely and appropriate corrective action is taken when weaknesses/violations are identified or when consumer complaints indicate significant deficiencies.

   - Audit/compliance review policies, procedures, and work papers.
   - Audit/compliance review reports and management responses.
   - Management reports.

Quantity of Risk Management

Conclusion: The quantity of risk is (low, moderate, high).

Perform only those procedures identified as areas of concern during the review of the "Quality of Risk Management."

Objective: Determine the bank's level of compliance with COPPA.

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

   - Data are collected, used and shared in accordance with the institution's Web site notice [16 CFR 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 [16 CFR 312.5(a)].

2. Through discussions with management and a review of policies and procedures, determine whether the 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].

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

4. Through testing or management's demonstration of the Web site or online service, verify that the financial institution does not condition 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 is reasonably necessary to participate in the activity [16 CFR 312.7].

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

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

- Complies with a parent's instructions concerning the collection, use, maintenance, or disclosure of his or her child's information. [16 CFR 312.6(a)(2) and 16 CFR 312.4(b)(2)(iv) and (vi)];

- Allows a parent to review any personal information collected from his or her child [16 CFR 312.6(a)(3)]; and

- Verifies that the person requesting information is a parent of the child [16 CFR 312.6 (a)(3)].

6. Complete the "COPPA Worksheet For Notices" by reviewing notices on the Web site or online service.

Conclusions

Objective: Prepare written conclusion summaries, discuss findings with the EIC, and communicate findings to management. If necessary, initiate corrective action when policies or internal controls are deficient or when violations of law or regulation are identified.

1. Summarize findings and violations from the preceding procedural steps to assess the bank's level of compliance with COPPA.

2. For those violations found to be significant or a pattern or practice, determine the root cause of violation(s) by identifying weaknesses in:

   - Internal controls.
   - Audit/independent compliance review.
   - Training.
   - Management oversight.

3. Determine whether a civil money penalty (CMP) or an enforcement action should be recommended (refer to the CMP matrix).

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

5. Form a conclusion about the reliability of the compliance management system for COPPA and provide conclusions to the examiner performing the Compliance Management System program.

6. Determine whether any items identified during this examination could materialize into supervisory concerns before the next on-site examination (considering whether the bank has plans to increase monitoring in the affected area, or anticipates changes in personnel, policy, outside auditors or consultants, or business strategy). If so, summarize your concerns and assess the potential risk to the bank.

7. Determine the impact on the aggregate quantity and direction of risk assessment for any concerns identified during the review. Examiners should refer to guidance provided under the OCC's large and community bank risk assessment programs.

   - Risk categories: compliance, transaction, and reputation risk.
   - Risk conclusions: high, moderate, or low.

- Risk direction: increasing, stable, or declining.

8. Provide, and discuss with, the EIC (and the supervisory office, if appropriate) conclusions, including:

   - A summary of violations and recommended CMPs/enforcement actions, if any.
   - Potential reimbursements.
   - Recommended corrective action.
   - The quantity of risk and quality of risk management.
   - Recommended matters requiring attention (MRA). MRA should cover practices that:
     – Deviate from sound fundamental principles and are likely to result in financial deterioration if not addressed.
     – Result in substantive noncompliance with laws.
   - MRA should discuss:
     – Causative factors contributing to the problem.
     – Consequences of inaction to the institution.
     – Management's commitment for corrective action.
     – The time frame and person(s) responsible for corrective action.

9. Discuss findings with management. Obtain commitment(s) for corrective action as needed. Include in the discussion:

   - The quality of risk management.
   - The quantity of risk (include a listing of all violations, as well as significant violations).
   - MRA(s).

10. As appropriate, prepare a brief comment for inclusion in the report of examination.

11. Prepare a memorandum summarizing work performed (e.g., sampling method used, internal control systems, scope of audit review, conclusions regarding audit, etc.) and update the work program with any information that will facilitate future examinations. Update the OCC database on all violations of law or regulation.

12. Organize and reference working papers in accordance with OCC guidance (PPM 5400-8).

Children's Online Privacy Protection Act Worksheet for Notices

Every "No" answer indicates a potential violation of the regulation or an internal control deficiency and must be fully explained in the work papers.

Web site Notice (16 CFR 312.4)	**Yes**	**No**
1. A Web site link is posted 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 Web site's information practices with regard to children, and is 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 [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 Web site [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 [16 CFR 312.4(b)(2)(iv)]: – 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; • 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 • That 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 – The notice states the procedures for doing so [16 CFR 312.4(b)(2)(vi)].		
4. The notice to a parent • States that the operator wishes to collect information from the child [16 CFR 312.4(c)(1)(i)(A)]. • Includes the information contained in the 16 CFR 312.4(b) Web site notice (see step 3 above) [16 CFR 312.4(c)(1)(i)]. • If 16 CFR 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 16 CFR 312.5(c)(3) and (4) apply.		

Children's Online Privacy Protection Act

Appendix B

Request Letter Enclosure

1. COPPA policies and procedures.

2. COPPA training materials.

3. COPPA compliance reports, audit reports, procedures, and management responses. Note: If the bank participates in an FTC-approved, self-regulatory program, provide a copy of the program and audit reports.

4. Complaints regarding the collection, sharing, or use of data from a child.

5. Copies of Web site notices since the last examination.

6. A list of data elements collected from a child and a description of how the data are used and protected.

7. A list of data elements collected from a child that are disclosed to third parties and any contracts or agreements governing the use of that information with those third parties.

8. A list of parental requests for personal information provided by their children.

9. A description of how parental permission is obtained and the method of verifying that the person providing consent is the child's parent.

Laws

15 USC 6501 et seq., Children's Online Privacy Protection Act

Regulations

16 CFR 312, Children's Online Privacy Protection Rule

OCC Issuances

Bulletin 2001-8, "Guidelines Establishing Standards for Safeguarding Customer Information," dated 02/05/01.

Bulletin 2001-26, "Privacy of Consumer Financial Information; 12 CFR 40," dated 05/25/01.

Bulletin 2001-31, Weblinking," dated 07/03/01.

Bulletin 2001-35, "Examination Procedures to Evaluate Compliance with Guidelines to Safeguard Customer Information," dated 07/18/01.

Advisory Letter 2001-08, "Authentication in an Electronic Banking Environment," dated 07/30/01.

CHILDREN'S ONLINE PRIVACY PROTECTION ACT

Children's Online Privacy Protection Act

Table of Contents

Children's Online Privacy Protection Act

Introduction

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 that is collected from children through Web sites 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 Web site(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.

Financial institutions that do not currently operate a Web site or online service directed to children, or do not have actual knowledge that they are collecting or maintaining personal information from a child online, are not subject to COPPA and will not be subject to COPPA examinations by the Office of the Comptroller of the Currency (OCC). However, financial institutions are urged to review their Web sites and their online information collection practices to ensure that they do not inadvertently trigger the provisions of this Act.

Definitions

"Child", "Children": (an) individual(s) under the age of 13.

"Personal information": 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 Web site 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 to the parent and on the Web site 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 and have deleted the personal information collected from his or 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).

Notice on the Web Site

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

An operator of a Web site or online service directed to children must post a link to a notice of its information practices with regard to children on its home page and at each area on the site or service where it collects personal information from any child. 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.

These links must be placed in a clear and prominent location on the home page of the Web site 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 that requires visitors to scroll down the 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 child through the Web site or online service;

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

- The way the operator uses, or may use, the personal information;

- A statement of 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 there is a prohibition against requiring, 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 has a right to 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 child can be made. 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's wishes to collect personal information from the parent's child;

- The requirement of the parent's consent for the collection, use, and disclosure of the information; and

- The way(s) the parent can provide consent.

Internal Uses [16 CFR 312.5(b)]

Financial institutions that use the personal information solely for internal purposes 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.

Disclosure to Others [16 CFR 312.5(b)]

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 requires a more reliable method of consent. The method used to obtain verifiable parental consent must be reasonably calculated, in light of available technology, to ensure that the person providing the consent is the child's parent. Methods that satisfy this requirement include:

- Obtaining a signed consent form from a parent via postal mail or facsimile;

- Accepting and verifying a parent's credit card number;

- Taking a parent's call, through a toll-free telephone number staffed by trained personnel;

- Receiving a parent's e-mail, accompanied by a digital signature; and

- Receiving an e-mail from a parent that is accompanied by a personal identification number (PIN) or password obtained through one of the methods mentioned above.

Disclosures to Third Parties [16 CFR 312.5(a)]

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 [16 CFR 312.5(a)]

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 [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 period 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 to, on a one-time basis, 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 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 Web site or online service is required to provide to a parent a means by which he or she can obtain any personal information collected from his or her child by that operator. 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. These methods might include requiring a parent to use a credit card in connection with a transaction; having a parent call a toll-free number staffed by trained personnel; using a digital certificate that uses public key technology; or using e-mail accompanied by a PIN or password.

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 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 any child.

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 Web site or online service that complies with FTC-approved, self-regulatory guidelines will receive a "safe harbor" from the requirements of COPPA and the regulation.

To be approved by the FTC, self-regulatory guidelines must include a requirement that operators subject to the guidelines implement substantially similar requirements that provide the same or greater protections for a child as the FTC regulation (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.

General Procedures

Objective: Determine the scope of the Children's Online Privacy Protection Act (COPPA) examination.

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

   - Is directed to children; or
   - Knowingly collects or maintains personal information from children.

   If the institution does not currently operate a Web site directed to children or knowingly collect information about them, the institution is not subject to COPPA, and no further examination for COPPA is necessary.

2. If the institution is subject to COPPA, determine whether it is participating in an FTC-approved, self-regulatory program (see 16 CFR 312.10). If it is, obtain a copy of the program and supporting documentation, such as reviews or audits, that demonstrate the institution's compliance with the program. If, under the self-regulatory program, an independent assessment found the institution in compliance with COPPA, or no assessment has yet been made, no further examination for COPPA is necessary. If, however, the independent assessment found the institution not in compliance with COPPA and the institution has not taken appropriate corrective action, continue with the procedures below.

3. If the institution is subject to COPPA and is not participating in an FTC-approved, self-regulatory program, continue with the procedures below.

4. From the examiner assigned the Compliance Management System program, obtain and review the following information to identify any previous or emerging problems that require follow-up:

   - Historical examination findings.
   - Complaint information from the bank and the OCC's Customer Assistance Group (CAG), and any CAG analytical reports, regarding the inappropriate collection, sharing, or use of data from a child.
   - Significant findings from the compliance audit.
   - Work papers from the prior examination.

5. Determine the following through early discussions with management:

   - Management supervision of compliance with COPPA, including responsiveness to, and corrective measures resulting from, consumer complaint activity.
   - Changes in processes, including forms, contracts, software programs, etc., since the previous examination.
   - Significant changes in policies, personnel, or controls.
   - Internal or external factors that could affect compliance with COPPA.
   - Whether applicable provisions of state laws and regulations are monitored and included in the bank's audit.

6. Complete the "Quality of Risk Management" procedures.

7. Complete appropriate sections of the "Quantity of Risk" procedures. The procedures performed in the "Quantity of Risk" section should address areas of concern identified during the review of "Quality of Risk Management."

8. Complete the "Conclusion Procedures."

Quality of Risk Management

Conclusion: The quality of risk management is (strong, satisfactory, weak).

Policy

Conclusion: The board (has/has not) established appropriate policies to ensure compliance with the Children's Online Privacy Protect Act.

Objective: Determine whether the bank has appropriate formal/informal policies to ensure compliance with COPPA.

1. Determine whether the board has adopted, and management has implemented adequate policies and procedures to maintain compliance with COPPA. Where appropriate, they should address:

   - Significant requirements of the law and the regulation.
   - Responsibilities and accountabilities of key personnel.
   - Training program.
   - Process for responding to changes in the law and the regulation.
   - Role of audit and compliance review.

2. Determine whether the board or an appropriate committee periodically reviews and approves compliance policies.

Processes

Conclusion: Management (has/has not) established effective processes to ensure compliance with COPPA.

Objective: Determine the reliance that can be placed on the bank's processes to prevent violations of COPPA.

1. Determine whether the bank's system for communicating the requirements of, and any subsequent changes to, COPPA is adequate to ensure ongoing compliance.

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

- Organization chart to determine who is responsible for the institution's compliance with COPPA;
- Process flow charts 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 Web site or online service;
- List of data elements collected from a child and a description of how the data are used and protected;
- List of data elements collected from a child that are disclosed to third parties and any contracts or agreements governing the use of that information with those third parties;
- Internal checklists, worksheets, and other review documents.

3. Assess the procedures used to ensure compliance when new online products are developed and operational changes are made.

Personnel

Conclusion: Bank management and personnel (do/do not) possess the required technical skills and knowledge to ensure compliance with COPPA.

Objective: Determine whether bank management and personnel possess sufficient knowledge and technical skills to manage and perform duties related to COPPA.

1. Assess bank management and personnel's knowledge and technical skills regarding COPPA based on conclusions developed while performing these procedures. Also consider:
   - Employee roles and responsibilities.
   - Training and experience.
   - Violations cited.
2. Review the bank's training program (materials, agendas, rosters, frequency, evaluation forms, etc.) and discuss with management to

determine how frequently and how well employees are trained regarding compliance with COPPA.

Controls

Conclusion: Management (has/has not) established effective control systems to ensure compliance with COPPA.

Objective: Determine the reliance that can be placed on the bank's control systems to detect and correct violations of COPPA, including practices and procedures performed by audit and compliance review.

1. Review audit and compliance review material, including working papers and reports, to determine whether:

   - The procedures address the COPPA provisions applicable to the institution;
   - The audits and reviews performed were reasonable and accurate;
   - The frequency of the compliance review is satisfactory;
   - Effective corrective action occurred in response to previously identified deficiencies; and
   - Deficiencies, their causes, and the effective corrective actions are consistently reported to management or the members of the board of directors.

2. Review the following documents and discuss with management to determine whether management information systems are sufficient and whether adequate practices are in place to ensure that timely and appropriate corrective action is taken when weaknesses/violations are identified or when consumer complaints indicate significant deficiencies.

   - Audit/compliance review policies, procedures, and work papers.
   - Audit/compliance review reports and management responses.
   - Management reports.

Quantity of Risk Management

Conclusion: The quantity of risk is (low, moderate, high).

Perform only those procedures identified as areas of concern during the review of the "Quality of Risk Management."

Objective: Determine the bank's level of compliance with COPPA.

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

   - Data are collected, used and shared in accordance with the institution's Web site notice [16 CFR 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 [16 CFR 312.5(a)].

2. Through discussions with management and a review of policies and procedures, determine whether the 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].

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

4. Through testing or management's demonstration of the Web site or online service, verify that the financial institution does not condition 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 is reasonably necessary to participate in the activity [16 CFR 312.7].

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

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

- Complies with a parent's instructions concerning the collection, use, maintenance, or disclosure of his or her child's information. [16 CFR 312.6(a)(2) and 16 CFR 312.4(b)(2)(iv) and (vi)];

- Allows a parent to review any personal information collected from his or her child [16 CFR 312.6(a)(3)]; and

- Verifies that the person requesting information is a parent of the child [16 CFR 312.6 (a)(3)].

6. Complete the "COPPA Worksheet For Notices" by reviewing notices on the Web site or online service.

Conclusions

Objective: Prepare written conclusion summaries, discuss findings with the EIC, and communicate findings to management. If necessary, initiate corrective action when policies or internal controls are deficient or when violations of law or regulation are identified.

1. Summarize findings and violations from the preceding procedural steps to assess the bank's level of compliance with COPPA.

2. For those violations found to be significant or a pattern or practice, determine the root cause of violation(s) by identifying weaknesses in:

   - Internal controls.
   - Audit/independent compliance review.
   - Training.
   - Management oversight.

3. Determine whether a civil money penalty (CMP) or an enforcement action should be recommended (refer to the CMP matrix).

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

5. Form a conclusion about the reliability of the compliance management system for COPPA and provide conclusions to the examiner performing the Compliance Management System program.

6. Determine whether any items identified during this examination could materialize into supervisory concerns before the next on-site examination (considering whether the bank has plans to increase monitoring in the affected area, or anticipates changes in personnel, policy, outside auditors or consultants, or business strategy). If so, summarize your concerns and assess the potential risk to the bank.

7. Determine the impact on the aggregate quantity and direction of risk assessment for any concerns identified during the review. Examiners should refer to guidance provided under the OCC's large and community bank risk assessment programs.

   - Risk categories: compliance, transaction, and reputation risk.
   - Risk conclusions: high, moderate, or low.

- Risk direction: increasing, stable, or declining.

8. Provide, and discuss with, the EIC (and the supervisory office, if appropriate) conclusions, including:

   - A summary of violations and recommended CMPs/enforcement actions, if any.
   - Potential reimbursements.
   - Recommended corrective action.
   - The quantity of risk and quality of risk management.
   - Recommended matters requiring attention (MRA). MRA should cover practices that:
     – Deviate from sound fundamental principles and are likely to result in financial deterioration if not addressed.
     – Result in substantive noncompliance with laws.
   - MRA should discuss:
     – Causative factors contributing to the problem.
     – Consequences of inaction to the institution.
     – Management's commitment for corrective action.
     – The time frame and person(s) responsible for corrective action.

9. Discuss findings with management. Obtain commitment(s) for corrective action as needed. Include in the discussion:

   - The quality of risk management.
   - The quantity of risk (include a listing of all violations, as well as significant violations).
   - MRA(s).

10. As appropriate, prepare a brief comment for inclusion in the report of examination.

11. Prepare a memorandum summarizing work performed (e.g., sampling method used, internal control systems, scope of audit review, conclusions regarding audit, etc.) and update the work program with any information that will facilitate future examinations. Update the OCC database on all violations of law or regulation.

12. Organize and reference working papers in accordance with OCC guidance (PPM 5400-8).

Children's Online Privacy Protection Act Worksheet for Notices

Every "No" answer indicates a potential violation of the regulation or an internal control deficiency and must be fully explained in the work papers.

Web site Notice (16 CFR 312.4)	**Yes**	**No**
1. A Web site link is posted 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 Web site's information practices with regard to children, and is 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 [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 Web site [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 [16 CFR 312.4(b)(2)(iv)]: – 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; • 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 • That 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 – The notice states the procedures for doing so [16 CFR 312.4(b)(2)(vi)].		
4. The notice to a parent • States that the operator wishes to collect information from the child [16 CFR 312.4(c)(1)(i)(A)]. • Includes the information contained in the 16 CFR 312.4(b) Web site notice (see step 3 above) [16 CFR 312.4(c)(1)(i)]. • If 16 CFR 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 16 CFR 312.5(c)(3) and (4) apply.		

Children's Online Privacy Protection Act

Appendix B

Request Letter Enclosure

1. COPPA policies and procedures.

2. COPPA training materials.

3. COPPA compliance reports, audit reports, procedures, and management responses. Note: If the bank participates in an FTC-approved, self-regulatory program, provide a copy of the program and audit reports.

4. Complaints regarding the collection, sharing, or use of data from a child.

5. Copies of Web site notices since the last examination.

6. A list of data elements collected from a child and a description of how the data are used and protected.

7. A list of data elements collected from a child that are disclosed to third parties and any contracts or agreements governing the use of that information with those third parties.

8. A list of parental requests for personal information provided by their children.

9. A description of how parental permission is obtained and the method of verifying that the person providing consent is the child's parent.

Laws

15 USC 6501 et seq., Children's Online Privacy Protection Act

Regulations

16 CFR 312, Children's Online Privacy Protection Rule

OCC Issuances

Bulletin 2001-8, "Guidelines Establishing Standards for Safeguarding Customer Information," dated 02/05/01.

Bulletin 2001-26, "Privacy of Consumer Financial Information; 12 CFR 40," dated 05/25/01.

Bulletin 2001-31, Weblinking," dated 07/03/01.

Bulletin 2001-35, "Examination Procedures to Evaluate Compliance with Guidelines to Safeguard Customer Information," dated 07/18/01.

Advisory Letter 2001-08, "Authentication in an Electronic Banking Environment," dated 07/30/01.

Children's Online Privacy Protection Act

Table of Contents

Children's Online Privacy Protection Act

Introduction

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 that is collected from children through Web sites 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 Web site(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.

Financial institutions that do not currently operate a Web site or online service directed to children, or do not have actual knowledge that they are collecting or maintaining personal information from a child online, are not subject to COPPA and will not be subject to COPPA examinations by the Office of the Comptroller of the Currency (OCC). However, financial institutions are urged to review their Web sites and their online information collection practices to ensure that they do not inadvertently trigger the provisions of this Act.

Definitions

"Child", "Children": (an) individual(s) under the age of 13.

"Personal information": 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 Web site 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 to the parent and on the Web site 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 and have deleted the personal information collected from his or 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).

Notice on the Web Site

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

An operator of a Web site or online service directed to children must post a link to a notice of its information practices with regard to children on its home page and at each area on the site or service where it collects personal information from any child. 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.

These links must be placed in a clear and prominent location on the home page of the Web site 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 that requires visitors to scroll down the 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 child through the Web site or online service;

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

- The way the operator uses, or may use, the personal information;

- A statement of 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 there is a prohibition against requiring, 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 has a right to 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 child can be made. 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's wishes to collect personal information from the parent's child;

- The requirement of the parent's consent for the collection, use, and disclosure of the information; and

- The way(s) the parent can provide consent.

Internal Uses [16 CFR 312.5(b)]

Financial institutions that use the personal information solely for internal purposes 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.

Disclosure to Others [16 CFR 312.5(b)]

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 requires a more reliable method of consent. The method used to obtain verifiable parental consent must be reasonably calculated, in light of available technology, to ensure that the person providing the consent is the child's parent. Methods that satisfy this requirement include:

- Obtaining a signed consent form from a parent via postal mail or facsimile;

- Accepting and verifying a parent's credit card number;

- Taking a parent's call, through a toll-free telephone number staffed by trained personnel;

- Receiving a parent's e-mail, accompanied by a digital signature; and

- Receiving an e-mail from a parent that is accompanied by a personal identification number (PIN) or password obtained through one of the methods mentioned above.

Disclosures to Third Parties [16 CFR 312.5(a)]

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 [16 CFR 312.5(a)]

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 [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 period 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 to, on a one-time basis, 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 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 Web site or online service is required to provide to a parent a means by which he or she can obtain any personal information collected from his or her child by that operator. 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. These methods might include requiring a parent to use a credit card in connection with a transaction; having a parent call a toll-free number staffed by trained personnel; using a digital certificate that uses public key technology; or using e-mail accompanied by a PIN or password.

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 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 any child.

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 Web site or online service that complies with FTC-approved, self-regulatory guidelines will receive a "safe harbor" from the requirements of COPPA and the regulation.

To be approved by the FTC, self-regulatory guidelines must include a requirement that operators subject to the guidelines implement substantially similar requirements that provide the same or greater protections for a child as the FTC regulation (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.

General Procedures

Objective: Determine the scope of the Children's Online Privacy Protection Act (COPPA) examination.

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

   - Is directed to children; or
   - Knowingly collects or maintains personal information from children.

   If the institution does not currently operate a Web site directed to children or knowingly collect information about them, the institution is not subject to COPPA, and no further examination for COPPA is necessary.

2. If the institution is subject to COPPA, determine whether it is participating in an FTC-approved, self-regulatory program (see 16 CFR 312.10). If it is, obtain a copy of the program and supporting documentation, such as reviews or audits, that demonstrate the institution's compliance with the program. If, under the self-regulatory program, an independent assessment found the institution in compliance with COPPA, or no assessment has yet been made, no further examination for COPPA is necessary. If, however, the independent assessment found the institution not in compliance with COPPA and the institution has not taken appropriate corrective action, continue with the procedures below.

3. If the institution is subject to COPPA and is not participating in an FTC-approved, self-regulatory program, continue with the procedures below.

4. From the examiner assigned the Compliance Management System program, obtain and review the following information to identify any previous or emerging problems that require follow-up:

   - Historical examination findings.
   - Complaint information from the bank and the OCC's Customer Assistance Group (CAG), and any CAG analytical reports, regarding the inappropriate collection, sharing, or use of data from a child.
   - Significant findings from the compliance audit.
   - Work papers from the prior examination.

5. Determine the following through early discussions with management:

   - Management supervision of compliance with COPPA, including responsiveness to, and corrective measures resulting from, consumer complaint activity.
   - Changes in processes, including forms, contracts, software programs, etc., since the previous examination.
   - Significant changes in policies, personnel, or controls.
   - Internal or external factors that could affect compliance with COPPA.
   - Whether applicable provisions of state laws and regulations are monitored and included in the bank's audit.

6. Complete the "Quality of Risk Management" procedures.

7. Complete appropriate sections of the "Quantity of Risk" procedures. The procedures performed in the "Quantity of Risk" section should address areas of concern identified during the review of "Quality of Risk Management."

8. Complete the "Conclusion Procedures."

Quality of Risk Management

Conclusion: The quality of risk management is (strong, satisfactory, weak).

Policy

Conclusion: The board (has/has not) established appropriate policies to ensure compliance with the Children's Online Privacy Protect Act.

Objective: Determine whether the bank has appropriate formal/informal policies to ensure compliance with COPPA.

1. Determine whether the board has adopted, and management has implemented adequate policies and procedures to maintain compliance with COPPA. Where appropriate, they should address:

   - Significant requirements of the law and the regulation.
   - Responsibilities and accountabilities of key personnel.
   - Training program.
   - Process for responding to changes in the law and the regulation.
   - Role of audit and compliance review.

2. Determine whether the board or an appropriate committee periodically reviews and approves compliance policies.

Processes

Conclusion: Management (has/has not) established effective processes to ensure compliance with COPPA.

Objective: Determine the reliance that can be placed on the bank's processes to prevent violations of COPPA.

1. Determine whether the bank's system for communicating the requirements of, and any subsequent changes to, COPPA is adequate to ensure ongoing compliance.

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

- Organization chart to determine who is responsible for the institution's compliance with COPPA;
- Process flow charts 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 Web site or online service;
- List of data elements collected from a child and a description of how the data are used and protected;
- List of data elements collected from a child that are disclosed to third parties and any contracts or agreements governing the use of that information with those third parties;
- Internal checklists, worksheets, and other review documents.

3. Assess the procedures used to ensure compliance when new online products are developed and operational changes are made.

Personnel

Conclusion: Bank management and personnel (do/do not) possess the required technical skills and knowledge to ensure compliance with COPPA.

Objective: Determine whether bank management and personnel possess sufficient knowledge and technical skills to manage and perform duties related to COPPA.

1. Assess bank management and personnel's knowledge and technical skills regarding COPPA based on conclusions developed while performing these procedures. Also consider:
   - Employee roles and responsibilities.
   - Training and experience.
   - Violations cited.
2. Review the bank's training program (materials, agendas, rosters, frequency, evaluation forms, etc.) and discuss with management to

determine how frequently and how well employees are trained regarding compliance with COPPA.

Controls

Conclusion: Management (has/has not) established effective control systems to ensure compliance with COPPA.

Objective: Determine the reliance that can be placed on the bank's control systems to detect and correct violations of COPPA, including practices and procedures performed by audit and compliance review.

1. Review audit and compliance review material, including working papers and reports, to determine whether:

   - The procedures address the COPPA provisions applicable to the institution;
   - The audits and reviews performed were reasonable and accurate;
   - The frequency of the compliance review is satisfactory;
   - Effective corrective action occurred in response to previously identified deficiencies; and
   - Deficiencies, their causes, and the effective corrective actions are consistently reported to management or the members of the board of directors.

2. Review the following documents and discuss with management to determine whether management information systems are sufficient and whether adequate practices are in place to ensure that timely and appropriate corrective action is taken when weaknesses/violations are identified or when consumer complaints indicate significant deficiencies.

   - Audit/compliance review policies, procedures, and work papers.
   - Audit/compliance review reports and management responses.
   - Management reports.

Quantity of Risk Management

Conclusion: The quantity of risk is (low, moderate, high).

Perform only those procedures identified as areas of concern during the review of the "Quality of Risk Management."

Objective: Determine the bank's level of compliance with COPPA.

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

   - Data are collected, used and shared in accordance with the institution's Web site notice [16 CFR 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 [16 CFR 312.5(a)].

2. Through discussions with management and a review of policies and procedures, determine whether the 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].

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

4. Through testing or management's demonstration of the Web site or online service, verify that the financial institution does not condition 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 is reasonably necessary to participate in the activity [16 CFR 312.7].

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

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

- Complies with a parent's instructions concerning the collection, use, maintenance, or disclosure of his or her child's information. [16 CFR 312.6(a)(2) and 16 CFR 312.4(b)(2)(iv) and (vi)];

- Allows a parent to review any personal information collected from his or her child [16 CFR 312.6(a)(3)]; and

- Verifies that the person requesting information is a parent of the child [16 CFR 312.6 (a)(3)].

6. Complete the "COPPA Worksheet For Notices" by reviewing notices on the Web site or online service.

Conclusions

Objective: Prepare written conclusion summaries, discuss findings with the EIC, and communicate findings to management. If necessary, initiate corrective action when policies or internal controls are deficient or when violations of law or regulation are identified.

1. Summarize findings and violations from the preceding procedural steps to assess the bank's level of compliance with COPPA.

2. For those violations found to be significant or a pattern or practice, determine the root cause of violation(s) by identifying weaknesses in:

   - Internal controls.
   - Audit/independent compliance review.
   - Training.
   - Management oversight.

3. Determine whether a civil money penalty (CMP) or an enforcement action should be recommended (refer to the CMP matrix).

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

5. Form a conclusion about the reliability of the compliance management system for COPPA and provide conclusions to the examiner performing the Compliance Management System program.

6. Determine whether any items identified during this examination could materialize into supervisory concerns before the next on-site examination (considering whether the bank has plans to increase monitoring in the affected area, or anticipates changes in personnel, policy, outside auditors or consultants, or business strategy). If so, summarize your concerns and assess the potential risk to the bank.

7. Determine the impact on the aggregate quantity and direction of risk assessment for any concerns identified during the review. Examiners should refer to guidance provided under the OCC's large and community bank risk assessment programs.

   - Risk categories: compliance, transaction, and reputation risk.
   - Risk conclusions: high, moderate, or low.

- Risk direction: increasing, stable, or declining.

8. Provide, and discuss with, the EIC (and the supervisory office, if appropriate) conclusions, including:

   - A summary of violations and recommended CMPs/enforcement actions, if any.
   - Potential reimbursements.
   - Recommended corrective action.
   - The quantity of risk and quality of risk management.
   - Recommended matters requiring attention (MRA). MRA should cover practices that:
     – Deviate from sound fundamental principles and are likely to result in financial deterioration if not addressed.
     – Result in substantive noncompliance with laws.
   - MRA should discuss:
     – Causative factors contributing to the problem.
     – Consequences of inaction to the institution.
     – Management's commitment for corrective action.
     – The time frame and person(s) responsible for corrective action.

9. Discuss findings with management. Obtain commitment(s) for corrective action as needed. Include in the discussion:

   - The quality of risk management.
   - The quantity of risk (include a listing of all violations, as well as significant violations).
   - MRA(s).

10. As appropriate, prepare a brief comment for inclusion in the report of examination.

11. Prepare a memorandum summarizing work performed (e.g., sampling method used, internal control systems, scope of audit review, conclusions regarding audit, etc.) and update the work program with any information that will facilitate future examinations. Update the OCC database on all violations of law or regulation.

12. Organize and reference working papers in accordance with OCC guidance (PPM 5400-8).

Children's Online Privacy Protection Act Worksheet for Notices

Every "No" answer indicates a potential violation of the regulation or an internal control deficiency and must be fully explained in the work papers.

Web site Notice (16 CFR 312.4)	**Yes**	**No**
1. A Web site link is posted 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 Web site's information practices with regard to children, and is 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 [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 Web site [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 [16 CFR 312.4(b)(2)(iv)]: – 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; • 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 • That 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 – The notice states the procedures for doing so [16 CFR 312.4(b)(2)(vi)].		
4. The notice to a parent • States that the operator wishes to collect information from the child [16 CFR 312.4(c)(1)(i)(A)]. • Includes the information contained in the 16 CFR 312.4(b) Web site notice (see step 3 above) [16 CFR 312.4(c)(1)(i)]. • If 16 CFR 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 16 CFR 312.5(c)(3) and (4) apply.		

Children's Online Privacy Protection Act

Appendix B

Request Letter Enclosure

1. COPPA policies and procedures.

2. COPPA training materials.

3. COPPA compliance reports, audit reports, procedures, and management responses. Note: If the bank participates in an FTC-approved, self-regulatory program, provide a copy of the program and audit reports.

4. Complaints regarding the collection, sharing, or use of data from a child.

5. Copies of Web site notices since the last examination.

6. A list of data elements collected from a child and a description of how the data are used and protected.

7. A list of data elements collected from a child that are disclosed to third parties and any contracts or agreements governing the use of that information with those third parties.

8. A list of parental requests for personal information provided by their children.

9. A description of how parental permission is obtained and the method of verifying that the person providing consent is the child's parent.

Laws

15 USC 6501 et seq., Children's Online Privacy Protection Act

Regulations

16 CFR 312, Children's Online Privacy Protection Rule

OCC Issuances

Bulletin 2001-8, "Guidelines Establishing Standards for Safeguarding Customer Information," dated 02/05/01.

Bulletin 2001-26, "Privacy of Consumer Financial Information; 12 CFR 40," dated 05/25/01.

Bulletin 2001-31, Weblinking," dated 07/03/01.

Bulletin 2001-35, "Examination Procedures to Evaluate Compliance with Guidelines to Safeguard Customer Information," dated 07/18/01.

Advisory Letter 2001-08, "Authentication in an Electronic Banking Environment," dated 07/30/01.

Comptroller of the Currency
Administrator of National Banks
US Department of the Treasury

OCC 2002-31

Subject: Children's Online Privacy Protection Act (COPPA)
Date: July 16, 2002

To: Chief Executive Officers and Compliance Officers of All National Banks, Department and Division Heads, and All Examining Personnel

Description: Examination Procedures

Attached are examination procedures for the Children's Online Privacy Protection Act (COPPA) that are effective immediately. COPPA addresses the collection, use, or disclosure of personal information that is collected from children through Web sites or other online services. Financial institutions that do not currently operate a Web site or online service directed to children or that do not have actual knowledge that they are collecting or maintaining personal information from a child online are not subject to COPPA and will not be subject to COPPA examinations by the OCC. However, financial institutions are urged to review their Web sites and their online information collection practices to ensure that they do not inadvertently trigger the provisions of this act.

The Federal Trade Commission issued a regulation, 16 CFR 312, implementing COPPA. It became effective on April 21, 2000.

For more information, contact your supervisory office or the Compliance Department at (202) 874-4428.

David G. Hammaker
Deputy Comptroller for Compliance

Related Links

- COPPA Examination Procedures

CHILDREN'S ONLINE PRIVACY PROTECTION ACT

Children's Online Privacy Protection Act

Table of Contents

Children's Online Privacy Protection Act

Introduction

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 that is collected from children through Web sites 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 Web site(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.

Financial institutions that do not currently operate a Web site or online service directed to children, or do not have actual knowledge that they are collecting or maintaining personal information from a child online, are not subject to COPPA and will not be subject to COPPA examinations by the Office of the Comptroller of the Currency (OCC). However, financial institutions are urged to review their Web sites and their online information collection practices to ensure that they do not inadvertently trigger the provisions of this Act.

Definitions

"Child", "Children": (an) individual(s) under the age of 13.

"Personal information": 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 Web site 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 to the parent and on the Web site 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 and have deleted the personal information collected from his or 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).

Notice on the Web Site

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

An operator of a Web site or online service directed to children must post a link to a notice of its information practices with regard to children on its home page and at each area on the site or service where it collects personal information from any child. 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.

These links must be placed in a clear and prominent location on the home page of the Web site 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 that requires visitors to scroll down the 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 child through the Web site or online service;

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

- The way the operator uses, or may use, the personal information;

- A statement of 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 there is a prohibition against requiring, 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 has a right to 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 child can be made. 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's wishes to collect personal information from the parent's child;

- The requirement of the parent's consent for the collection, use, and disclosure of the information; and

- The way(s) the parent can provide consent.

Internal Uses [16 CFR 312.5(b)]

Financial institutions that use the personal information solely for internal purposes 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.

Disclosure to Others [16 CFR 312.5(b)]

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 requires a more reliable method of consent. The method used to obtain verifiable parental consent must be reasonably calculated, in light of available technology, to ensure that the person providing the consent is the child's parent. Methods that satisfy this requirement include:

- Obtaining a signed consent form from a parent via postal mail or facsimile;

- Accepting and verifying a parent's credit card number;

- Taking a parent's call, through a toll-free telephone number staffed by trained personnel;

- Receiving a parent's e-mail, accompanied by a digital signature; and

- Receiving an e-mail from a parent that is accompanied by a personal identification number (PIN) or password obtained through one of the methods mentioned above.

Disclosures to Third Parties [16 CFR 312.5(a)]

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 [16 CFR 312.5(a)]

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 [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 period 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 to, on a one-time basis, 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 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 Web site or online service is required to provide to a parent a means by which he or she can obtain any personal information collected from his or her child by that operator. 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. These methods might include requiring a parent to use a credit card in connection with a transaction; having a parent call a toll-free number staffed by trained personnel; using a digital certificate that uses public key technology; or using e-mail accompanied by a PIN or password.

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 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 any child.

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 Web site or online service that complies with FTC-approved, self-regulatory guidelines will receive a "safe harbor" from the requirements of COPPA and the regulation.

To be approved by the FTC, self-regulatory guidelines must include a requirement that operators subject to the guidelines implement substantially similar requirements that provide the same or greater protections for a child as the FTC regulation (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.

General Procedures

Objective: Determine the scope of the Children's Online Privacy Protection Act (COPPA) examination.

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

   - Is directed to children; or
   - Knowingly collects or maintains personal information from children.

   If the institution does not currently operate a Web site directed to children or knowingly collect information about them, the institution is not subject to COPPA, and no further examination for COPPA is necessary.

2. If the institution is subject to COPPA, determine whether it is participating in an FTC-approved, self-regulatory program (see 16 CFR 312.10). If it is, obtain a copy of the program and supporting documentation, such as reviews or audits, that demonstrate the institution's compliance with the program. If, under the self-regulatory program, an independent assessment found the institution in compliance with COPPA, or no assessment has yet been made, no further examination for COPPA is necessary. If, however, the independent assessment found the institution not in compliance with COPPA and the institution has not taken appropriate corrective action, continue with the procedures below.

3. If the institution is subject to COPPA and is not participating in an FTC-approved, self-regulatory program, continue with the procedures below.

4. From the examiner assigned the Compliance Management System program, obtain and review the following information to identify any previous or emerging problems that require follow-up:

   - Historical examination findings.
   - Complaint information from the bank and the OCC's Customer Assistance Group (CAG), and any CAG analytical reports, regarding the inappropriate collection, sharing, or use of data from a child.
   - Significant findings from the compliance audit.
   - Work papers from the prior examination.

5. Determine the following through early discussions with management:

   - Management supervision of compliance with COPPA, including responsiveness to, and corrective measures resulting from, consumer complaint activity.
   - Changes in processes, including forms, contracts, software programs, etc., since the previous examination.
   - Significant changes in policies, personnel, or controls.
   - Internal or external factors that could affect compliance with COPPA.
   - Whether applicable provisions of state laws and regulations are monitored and included in the bank's audit.

6. Complete the "Quality of Risk Management" procedures.

7. Complete appropriate sections of the "Quantity of Risk" procedures. The procedures performed in the "Quantity of Risk" section should address areas of concern identified during the review of "Quality of Risk Management."

8. Complete the "Conclusion Procedures."

Quality of Risk Management

Conclusion: The quality of risk management is (strong, satisfactory, weak).

Policy

Conclusion: The board (has/has not) established appropriate policies to ensure compliance with the Children's Online Privacy Protect Act.

Objective: Determine whether the bank has appropriate formal/informal policies to ensure compliance with COPPA.

1. Determine whether the board has adopted, and management has implemented adequate policies and procedures to maintain compliance with COPPA. Where appropriate, they should address:

   - Significant requirements of the law and the regulation.
   - Responsibilities and accountabilities of key personnel.
   - Training program.
   - Process for responding to changes in the law and the regulation.
   - Role of audit and compliance review.

2. Determine whether the board or an appropriate committee periodically reviews and approves compliance policies.

Processes

Conclusion: Management (has/has not) established effective processes to ensure compliance with COPPA.

Objective: Determine the reliance that can be placed on the bank's processes to prevent violations of COPPA.

1. Determine whether the bank's system for communicating the requirements of, and any subsequent changes to, COPPA is adequate to ensure ongoing compliance.

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

- Organization chart to determine who is responsible for the institution's compliance with COPPA;
- Process flow charts 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 Web site or online service;
- List of data elements collected from a child and a description of how the data are used and protected;
- List of data elements collected from a child that are disclosed to third parties and any contracts or agreements governing the use of that information with those third parties;
- Internal checklists, worksheets, and other review documents.

3. Assess the procedures used to ensure compliance when new online products are developed and operational changes are made.

Personnel

Conclusion: Bank management and personnel (do/do not) possess the required technical skills and knowledge to ensure compliance with COPPA.

Objective: Determine whether bank management and personnel possess sufficient knowledge and technical skills to manage and perform duties related to COPPA.

1. Assess bank management and personnel's knowledge and technical skills regarding COPPA based on conclusions developed while performing these procedures. Also consider:
   - Employee roles and responsibilities.
   - Training and experience.
   - Violations cited.
2. Review the bank's training program (materials, agendas, rosters, frequency, evaluation forms, etc.) and discuss with management to

determine how frequently and how well employees are trained regarding compliance with COPPA.

Controls

Conclusion: Management (has/has not) established effective control systems to ensure compliance with COPPA.

Objective: Determine the reliance that can be placed on the bank's control systems to detect and correct violations of COPPA, including practices and procedures performed by audit and compliance review.

1. Review audit and compliance review material, including working papers and reports, to determine whether:

   - The procedures address the COPPA provisions applicable to the institution;
   - The audits and reviews performed were reasonable and accurate;
   - The frequency of the compliance review is satisfactory;
   - Effective corrective action occurred in response to previously identified deficiencies; and
   - Deficiencies, their causes, and the effective corrective actions are consistently reported to management or the members of the board of directors.

2. Review the following documents and discuss with management to determine whether management information systems are sufficient and whether adequate practices are in place to ensure that timely and appropriate corrective action is taken when weaknesses/violations are identified or when consumer complaints indicate significant deficiencies.

   - Audit/compliance review policies, procedures, and work papers.
   - Audit/compliance review reports and management responses.
   - Management reports.

Quantity of Risk Management

Conclusion: The quantity of risk is (low, moderate, high).

Perform only those procedures identified as areas of concern during the review of the "Quality of Risk Management."

Objective: Determine the bank's level of compliance with COPPA.

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

   - Data are collected, used and shared in accordance with the institution's Web site notice [16 CFR 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 [16 CFR 312.5(a)].

2. Through discussions with management and a review of policies and procedures, determine whether the 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].

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

4. Through testing or management's demonstration of the Web site or online service, verify that the financial institution does not condition 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 is reasonably necessary to participate in the activity [16 CFR 312.7].

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

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

- Complies with a parent's instructions concerning the collection, use, maintenance, or disclosure of his or her child's information. [16 CFR 312.6(a)(2) and 16 CFR 312.4(b)(2)(iv) and (vi)];

- Allows a parent to review any personal information collected from his or her child [16 CFR 312.6(a)(3)]; and

- Verifies that the person requesting information is a parent of the child [16 CFR 312.6 (a)(3)].

6. Complete the "COPPA Worksheet For Notices" by reviewing notices on the Web site or online service.

Conclusions

Objective: Prepare written conclusion summaries, discuss findings with the EIC, and communicate findings to management. If necessary, initiate corrective action when policies or internal controls are deficient or when violations of law or regulation are identified.

1. Summarize findings and violations from the preceding procedural steps to assess the bank's level of compliance with COPPA.

2. For those violations found to be significant or a pattern or practice, determine the root cause of violation(s) by identifying weaknesses in:

   - Internal controls.
   - Audit/independent compliance review.
   - Training.
   - Management oversight.

3. Determine whether a civil money penalty (CMP) or an enforcement action should be recommended (refer to the CMP matrix).

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

5. Form a conclusion about the reliability of the compliance management system for COPPA and provide conclusions to the examiner performing the Compliance Management System program.

6. Determine whether any items identified during this examination could materialize into supervisory concerns before the next on-site examination (considering whether the bank has plans to increase monitoring in the affected area, or anticipates changes in personnel, policy, outside auditors or consultants, or business strategy). If so, summarize your concerns and assess the potential risk to the bank.

7. Determine the impact on the aggregate quantity and direction of risk assessment for any concerns identified during the review. Examiners should refer to guidance provided under the OCC's large and community bank risk assessment programs.

   - Risk categories: compliance, transaction, and reputation risk.
   - Risk conclusions: high, moderate, or low.

- Risk direction: increasing, stable, or declining.

8. Provide, and discuss with, the EIC (and the supervisory office, if appropriate) conclusions, including:

   - A summary of violations and recommended CMPs/enforcement actions, if any.
   - Potential reimbursements.
   - Recommended corrective action.
   - The quantity of risk and quality of risk management.
   - Recommended matters requiring attention (MRA). MRA should cover practices that:
     – Deviate from sound fundamental principles and are likely to result in financial deterioration if not addressed.
     – Result in substantive noncompliance with laws.
   - MRA should discuss:
     – Causative factors contributing to the problem.
     – Consequences of inaction to the institution.
     – Management's commitment for corrective action.
     – The time frame and person(s) responsible for corrective action.

9. Discuss findings with management. Obtain commitment(s) for corrective action as needed. Include in the discussion:

   - The quality of risk management.
   - The quantity of risk (include a listing of all violations, as well as significant violations).
   - MRA(s).

10. As appropriate, prepare a brief comment for inclusion in the report of examination.

11. Prepare a memorandum summarizing work performed (e.g., sampling method used, internal control systems, scope of audit review, conclusions regarding audit, etc.) and update the work program with any information that will facilitate future examinations. Update the OCC database on all violations of law or regulation.

12. Organize and reference working papers in accordance with OCC guidance (PPM 5400-8).

Children's Online Privacy Protection Act Worksheet for Notices

Every "No" answer indicates a potential violation of the regulation or an internal control deficiency and must be fully explained in the work papers.

Web site Notice (16 CFR 312.4)	**Yes**	**No**
1. A Web site link is posted 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 Web site's information practices with regard to children, and is 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 [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 Web site [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 [16 CFR 312.4(b)(2)(iv)]: – 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; • 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 • That 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 – The notice states the procedures for doing so [16 CFR 312.4(b)(2)(vi)].		
4. The notice to a parent • States that the operator wishes to collect information from the child [16 CFR 312.4(c)(1)(i)(A)]. • Includes the information contained in the 16 CFR 312.4(b) Web site notice (see step 3 above) [16 CFR 312.4(c)(1)(i)]. • If 16 CFR 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 16 CFR 312.5(c)(3) and (4) apply.		

Children's Online Privacy Protection Act

Appendix B

Request Letter Enclosure

1. COPPA policies and procedures.

2. COPPA training materials.

3. COPPA compliance reports, audit reports, procedures, and management responses. Note: If the bank participates in an FTC-approved, self-regulatory program, provide a copy of the program and audit reports.

4. Complaints regarding the collection, sharing, or use of data from a child.

5. Copies of Web site notices since the last examination.

6. A list of data elements collected from a child and a description of how the data are used and protected.

7. A list of data elements collected from a child that are disclosed to third parties and any contracts or agreements governing the use of that information with those third parties.

8. A list of parental requests for personal information provided by their children.

9. A description of how parental permission is obtained and the method of verifying that the person providing consent is the child's parent.

Laws

15 USC 6501 et seq., Children's Online Privacy Protection Act

Regulations

16 CFR 312, Children's Online Privacy Protection Rule

OCC Issuances

Bulletin 2001-8, "Guidelines Establishing Standards for Safeguarding Customer Information," dated 02/05/01.

Bulletin 2001-26, "Privacy of Consumer Financial Information; 12 CFR 40," dated 05/25/01.

Bulletin 2001-31, Weblinking," dated 07/03/01.

Bulletin 2001-35, "Examination Procedures to Evaluate Compliance with Guidelines to Safeguard Customer Information," dated 07/18/01.

Advisory Letter 2001-08, "Authentication in an Electronic Banking Environment," dated 07/30/01.

CHILDREN'S ONLINE PRIVACY PROTECTION ACT

Children's Online Privacy Protection Act

Table of Contents

Children's Online Privacy Protection Act

Introduction

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 that is collected from children through Web sites 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 Web site(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.

Financial institutions that do not currently operate a Web site or online service directed to children, or do not have actual knowledge that they are collecting or maintaining personal information from a child online, are not subject to COPPA and will not be subject to COPPA examinations by the Office of the Comptroller of the Currency (OCC). However, financial institutions are urged to review their Web sites and their online information collection practices to ensure that they do not inadvertently trigger the provisions of this Act.

Definitions

"Child", "Children": (an) individual(s) under the age of 13.

"Personal information": 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 Web site 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 to the parent and on the Web site 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 and have deleted the personal information collected from his or 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).

Notice on the Web Site

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

An operator of a Web site or online service directed to children must post a link to a notice of its information practices with regard to children on its home page and at each area on the site or service where it collects personal information from any child. 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.

These links must be placed in a clear and prominent location on the home page of the Web site 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 that requires visitors to scroll down the 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 child through the Web site or online service;

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

- The way the operator uses, or may use, the personal information;

- A statement of 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 there is a prohibition against requiring, 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 has a right to 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 child can be made. 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's wishes to collect personal information from the parent's child;

- The requirement of the parent's consent for the collection, use, and disclosure of the information; and

- The way(s) the parent can provide consent.

Internal Uses [16 CFR 312.5(b)]

Financial institutions that use the personal information solely for internal purposes 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.

Disclosure to Others [16 CFR 312.5(b)]

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 requires a more reliable method of consent. The method used to obtain verifiable parental consent must be reasonably calculated, in light of available technology, to ensure that the person providing the consent is the child's parent. Methods that satisfy this requirement include:

- Obtaining a signed consent form from a parent via postal mail or facsimile;

- Accepting and verifying a parent's credit card number;

- Taking a parent's call, through a toll-free telephone number staffed by trained personnel;

- Receiving a parent's e-mail, accompanied by a digital signature; and

- Receiving an e-mail from a parent that is accompanied by a personal identification number (PIN) or password obtained through one of the methods mentioned above.

Disclosures to Third Parties [16 CFR 312.5(a)]

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 [16 CFR 312.5(a)]

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 [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 period 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 to, on a one-time basis, 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 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 Web site or online service is required to provide to a parent a means by which he or she can obtain any personal information collected from his or her child by that operator. 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. These methods might include requiring a parent to use a credit card in connection with a transaction; having a parent call a toll-free number staffed by trained personnel; using a digital certificate that uses public key technology; or using e-mail accompanied by a PIN or password.

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 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 any child.

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 Web site or online service that complies with FTC-approved, self-regulatory guidelines will receive a "safe harbor" from the requirements of COPPA and the regulation.

To be approved by the FTC, self-regulatory guidelines must include a requirement that operators subject to the guidelines implement substantially similar requirements that provide the same or greater protections for a child as the FTC regulation (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.

General Procedures

Objective: Determine the scope of the Children's Online Privacy Protection Act (COPPA) examination.

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

   - Is directed to children; or
   - Knowingly collects or maintains personal information from children.

   If the institution does not currently operate a Web site directed to children or knowingly collect information about them, the institution is not subject to COPPA, and no further examination for COPPA is necessary.

2. If the institution is subject to COPPA, determine whether it is participating in an FTC-approved, self-regulatory program (see 16 CFR 312.10). If it is, obtain a copy of the program and supporting documentation, such as reviews or audits, that demonstrate the institution's compliance with the program. If, under the self-regulatory program, an independent assessment found the institution in compliance with COPPA, or no assessment has yet been made, no further examination for COPPA is necessary. If, however, the independent assessment found the institution not in compliance with COPPA and the institution has not taken appropriate corrective action, continue with the procedures below.

3. If the institution is subject to COPPA and is not participating in an FTC-approved, self-regulatory program, continue with the procedures below.

4. From the examiner assigned the Compliance Management System program, obtain and review the following information to identify any previous or emerging problems that require follow-up:

   - Historical examination findings.
   - Complaint information from the bank and the OCC's Customer Assistance Group (CAG), and any CAG analytical reports, regarding the inappropriate collection, sharing, or use of data from a child.
   - Significant findings from the compliance audit.
   - Work papers from the prior examination.

5. Determine the following through early discussions with management:

   - Management supervision of compliance with COPPA, including responsiveness to, and corrective measures resulting from, consumer complaint activity.
   - Changes in processes, including forms, contracts, software programs, etc., since the previous examination.
   - Significant changes in policies, personnel, or controls.
   - Internal or external factors that could affect compliance with COPPA.
   - Whether applicable provisions of state laws and regulations are monitored and included in the bank's audit.

6. Complete the "Quality of Risk Management" procedures.

7. Complete appropriate sections of the "Quantity of Risk" procedures. The procedures performed in the "Quantity of Risk" section should address areas of concern identified during the review of "Quality of Risk Management."

8. Complete the "Conclusion Procedures."

Quality of Risk Management

Conclusion: The quality of risk management is (strong, satisfactory, weak).

Policy

Conclusion: The board (has/has not) established appropriate policies to ensure compliance with the Children's Online Privacy Protect Act.

Objective: Determine whether the bank has appropriate formal/informal policies to ensure compliance with COPPA.

1. Determine whether the board has adopted, and management has implemented adequate policies and procedures to maintain compliance with COPPA. Where appropriate, they should address:

   - Significant requirements of the law and the regulation.
   - Responsibilities and accountabilities of key personnel.
   - Training program.
   - Process for responding to changes in the law and the regulation.
   - Role of audit and compliance review.

2. Determine whether the board or an appropriate committee periodically reviews and approves compliance policies.

Processes

Conclusion: Management (has/has not) established effective processes to ensure compliance with COPPA.

Objective: Determine the reliance that can be placed on the bank's processes to prevent violations of COPPA.

1. Determine whether the bank's system for communicating the requirements of, and any subsequent changes to, COPPA is adequate to ensure ongoing compliance.

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

- Organization chart to determine who is responsible for the institution's compliance with COPPA;
- Process flow charts 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 Web site or online service;
- List of data elements collected from a child and a description of how the data are used and protected;
- List of data elements collected from a child that are disclosed to third parties and any contracts or agreements governing the use of that information with those third parties;
- Internal checklists, worksheets, and other review documents.

3. Assess the procedures used to ensure compliance when new online products are developed and operational changes are made.

Personnel

Conclusion: Bank management and personnel (do/do not) possess the required technical skills and knowledge to ensure compliance with COPPA.

Objective: Determine whether bank management and personnel possess sufficient knowledge and technical skills to manage and perform duties related to COPPA.

1. Assess bank management and personnel's knowledge and technical skills regarding COPPA based on conclusions developed while performing these procedures. Also consider:
   - Employee roles and responsibilities.
   - Training and experience.
   - Violations cited.
2. Review the bank's training program (materials, agendas, rosters, frequency, evaluation forms, etc.) and discuss with management to

determine how frequently and how well employees are trained regarding compliance with COPPA.

Controls

Conclusion: Management (has/has not) established effective control systems to ensure compliance with COPPA.

Objective: Determine the reliance that can be placed on the bank's control systems to detect and correct violations of COPPA, including practices and procedures performed by audit and compliance review.

1. Review audit and compliance review material, including working papers and reports, to determine whether:

   - The procedures address the COPPA provisions applicable to the institution;
   - The audits and reviews performed were reasonable and accurate;
   - The frequency of the compliance review is satisfactory;
   - Effective corrective action occurred in response to previously identified deficiencies; and
   - Deficiencies, their causes, and the effective corrective actions are consistently reported to management or the members of the board of directors.

2. Review the following documents and discuss with management to determine whether management information systems are sufficient and whether adequate practices are in place to ensure that timely and appropriate corrective action is taken when weaknesses/violations are identified or when consumer complaints indicate significant deficiencies.

   - Audit/compliance review policies, procedures, and work papers.
   - Audit/compliance review reports and management responses.
   - Management reports.

Quantity of Risk Management

Conclusion: The quantity of risk is (low, moderate, high).

Perform only those procedures identified as areas of concern during the review of the "Quality of Risk Management."

Objective: Determine the bank's level of compliance with COPPA.

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

   - Data are collected, used and shared in accordance with the institution's Web site notice [16 CFR 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 [16 CFR 312.5(a)].

2. Through discussions with management and a review of policies and procedures, determine whether the 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].

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

4. Through testing or management's demonstration of the Web site or online service, verify that the financial institution does not condition 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 is reasonably necessary to participate in the activity [16 CFR 312.7].

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

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

- Complies with a parent's instructions concerning the collection, use, maintenance, or disclosure of his or her child's information. [16 CFR 312.6(a)(2) and 16 CFR 312.4(b)(2)(iv) and (vi)];

- Allows a parent to review any personal information collected from his or her child [16 CFR 312.6(a)(3)]; and

- Verifies that the person requesting information is a parent of the child [16 CFR 312.6 (a)(3)].

6. Complete the "COPPA Worksheet For Notices" by reviewing notices on the Web site or online service.

Conclusions

Objective: Prepare written conclusion summaries, discuss findings with the EIC, and communicate findings to management. If necessary, initiate corrective action when policies or internal controls are deficient or when violations of law or regulation are identified.

1. Summarize findings and violations from the preceding procedural steps to assess the bank's level of compliance with COPPA.

2. For those violations found to be significant or a pattern or practice, determine the root cause of violation(s) by identifying weaknesses in:

   - Internal controls.
   - Audit/independent compliance review.
   - Training.
   - Management oversight.

3. Determine whether a civil money penalty (CMP) or an enforcement action should be recommended (refer to the CMP matrix).

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

5. Form a conclusion about the reliability of the compliance management system for COPPA and provide conclusions to the examiner performing the Compliance Management System program.

6. Determine whether any items identified during this examination could materialize into supervisory concerns before the next on-site examination (considering whether the bank has plans to increase monitoring in the affected area, or anticipates changes in personnel, policy, outside auditors or consultants, or business strategy). If so, summarize your concerns and assess the potential risk to the bank.

7. Determine the impact on the aggregate quantity and direction of risk assessment for any concerns identified during the review. Examiners should refer to guidance provided under the OCC's large and community bank risk assessment programs.

   - Risk categories: compliance, transaction, and reputation risk.
   - Risk conclusions: high, moderate, or low.

- Risk direction: increasing, stable, or declining.

8. Provide, and discuss with, the EIC (and the supervisory office, if appropriate) conclusions, including:

   - A summary of violations and recommended CMPs/enforcement actions, if any.
   - Potential reimbursements.
   - Recommended corrective action.
   - The quantity of risk and quality of risk management.
   - Recommended matters requiring attention (MRA). MRA should cover practices that:
     – Deviate from sound fundamental principles and are likely to result in financial deterioration if not addressed.
     – Result in substantive noncompliance with laws.
   - MRA should discuss:
     – Causative factors contributing to the problem.
     – Consequences of inaction to the institution.
     – Management's commitment for corrective action.
     – The time frame and person(s) responsible for corrective action.

9. Discuss findings with management. Obtain commitment(s) for corrective action as needed. Include in the discussion:

   - The quality of risk management.
   - The quantity of risk (include a listing of all violations, as well as significant violations).
   - MRA(s).

10. As appropriate, prepare a brief comment for inclusion in the report of examination.

11. Prepare a memorandum summarizing work performed (e.g., sampling method used, internal control systems, scope of audit review, conclusions regarding audit, etc.) and update the work program with any information that will facilitate future examinations. Update the OCC database on all violations of law or regulation.

12. Organize and reference working papers in accordance with OCC guidance (PPM 5400-8).

Children's Online Privacy Protection Act Worksheet for Notices

Every "No" answer indicates a potential violation of the regulation or an internal control deficiency and must be fully explained in the work papers.

Web site Notice (16 CFR 312.4)	**Yes**	**No**
1. A Web site link is posted 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 Web site's information practices with regard to children, and is 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 [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 Web site [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 [16 CFR 312.4(b)(2)(iv)]: – 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; • 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 • That 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 – The notice states the procedures for doing so [16 CFR 312.4(b)(2)(vi)].		
4. The notice to a parent • States that the operator wishes to collect information from the child [16 CFR 312.4(c)(1)(i)(A)]. • Includes the information contained in the 16 CFR 312.4(b) Web site notice (see step 3 above) [16 CFR 312.4(c)(1)(i)]. • If 16 CFR 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 16 CFR 312.5(c)(3) and (4) apply.		

Children's Online Privacy Protection Act

Appendix B

Request Letter Enclosure

1. COPPA policies and procedures.

2. COPPA training materials.

3. COPPA compliance reports, audit reports, procedures, and management responses. Note: If the bank participates in an FTC-approved, self-regulatory program, provide a copy of the program and audit reports.

4. Complaints regarding the collection, sharing, or use of data from a child.

5. Copies of Web site notices since the last examination.

6. A list of data elements collected from a child and a description of how the data are used and protected.

7. A list of data elements collected from a child that are disclosed to third parties and any contracts or agreements governing the use of that information with those third parties.

8. A list of parental requests for personal information provided by their children.

9. A description of how parental permission is obtained and the method of verifying that the person providing consent is the child's parent.

Laws

15 USC 6501 et seq., Children's Online Privacy Protection Act

Regulations

16 CFR 312, Children's Online Privacy Protection Rule

OCC Issuances

Bulletin 2001-8, "Guidelines Establishing Standards for Safeguarding Customer Information," dated 02/05/01.

Bulletin 2001-26, "Privacy of Consumer Financial Information; 12 CFR 40," dated 05/25/01.

Bulletin 2001-31, Weblinking," dated 07/03/01.

Bulletin 2001-35, "Examination Procedures to Evaluate Compliance with Guidelines to Safeguard Customer Information," dated 07/18/01.

Advisory Letter 2001-08, "Authentication in an Electronic Banking Environment," dated 07/30/01.

CHILDREN'S ONLINE PRIVACY PROTECTION ACT

Children's Online Privacy Protection Act

Table of Contents

Children's Online Privacy Protection Act

Introduction

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 that is collected from children through Web sites 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 Web site(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.

Financial institutions that do not currently operate a Web site or online service directed to children, or do not have actual knowledge that they are collecting or maintaining personal information from a child online, are not subject to COPPA and will not be subject to COPPA examinations by the Office of the Comptroller of the Currency (OCC). However, financial institutions are urged to review their Web sites and their online information collection practices to ensure that they do not inadvertently trigger the provisions of this Act.

Definitions

"Child", "Children": (an) individual(s) under the age of 13.

"Personal information": 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 Web site 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 to the parent and on the Web site 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 and have deleted the personal information collected from his or 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).

Notice on the Web Site

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

An operator of a Web site or online service directed to children must post a link to a notice of its information practices with regard to children on its home page and at each area on the site or service where it collects personal information from any child. 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.

These links must be placed in a clear and prominent location on the home page of the Web site 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 that requires visitors to scroll down the 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 child through the Web site or online service;

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

- The way the operator uses, or may use, the personal information;

- A statement of 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 there is a prohibition against requiring, 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 has a right to 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 child can be made. 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's wishes to collect personal information from the parent's child;

- The requirement of the parent's consent for the collection, use, and disclosure of the information; and

- The way(s) the parent can provide consent.

Internal Uses [16 CFR 312.5(b)]

Financial institutions that use the personal information solely for internal purposes 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.

Disclosure to Others [16 CFR 312.5(b)]

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 requires a more reliable method of consent. The method used to obtain verifiable parental consent must be reasonably calculated, in light of available technology, to ensure that the person providing the consent is the child's parent. Methods that satisfy this requirement include:

- Obtaining a signed consent form from a parent via postal mail or facsimile;

- Accepting and verifying a parent's credit card number;

- Taking a parent's call, through a toll-free telephone number staffed by trained personnel;

- Receiving a parent's e-mail, accompanied by a digital signature; and

- Receiving an e-mail from a parent that is accompanied by a personal identification number (PIN) or password obtained through one of the methods mentioned above.

Disclosures to Third Parties [16 CFR 312.5(a)]

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 [16 CFR 312.5(a)]

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 [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 period 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 to, on a one-time basis, 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 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 Web site or online service is required to provide to a parent a means by which he or she can obtain any personal information collected from his or her child by that operator. 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. These methods might include requiring a parent to use a credit card in connection with a transaction; having a parent call a toll-free number staffed by trained personnel; using a digital certificate that uses public key technology; or using e-mail accompanied by a PIN or password.

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 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 any child.

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 Web site or online service that complies with FTC-approved, self-regulatory guidelines will receive a "safe harbor" from the requirements of COPPA and the regulation.

To be approved by the FTC, self-regulatory guidelines must include a requirement that operators subject to the guidelines implement substantially similar requirements that provide the same or greater protections for a child as the FTC regulation (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.

General Procedures

Objective: Determine the scope of the Children's Online Privacy Protection Act (COPPA) examination.

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

   - Is directed to children; or
   - Knowingly collects or maintains personal information from children.

   If the institution does not currently operate a Web site directed to children or knowingly collect information about them, the institution is not subject to COPPA, and no further examination for COPPA is necessary.

2. If the institution is subject to COPPA, determine whether it is participating in an FTC-approved, self-regulatory program (see 16 CFR 312.10). If it is, obtain a copy of the program and supporting documentation, such as reviews or audits, that demonstrate the institution's compliance with the program. If, under the self-regulatory program, an independent assessment found the institution in compliance with COPPA, or no assessment has yet been made, no further examination for COPPA is necessary. If, however, the independent assessment found the institution not in compliance with COPPA and the institution has not taken appropriate corrective action, continue with the procedures below.

3. If the institution is subject to COPPA and is not participating in an FTC-approved, self-regulatory program, continue with the procedures below.

4. From the examiner assigned the Compliance Management System program, obtain and review the following information to identify any previous or emerging problems that require follow-up:

   - Historical examination findings.
   - Complaint information from the bank and the OCC's Customer Assistance Group (CAG), and any CAG analytical reports, regarding the inappropriate collection, sharing, or use of data from a child.
   - Significant findings from the compliance audit.
   - Work papers from the prior examination.

5. Determine the following through early discussions with management:

   - Management supervision of compliance with COPPA, including responsiveness to, and corrective measures resulting from, consumer complaint activity.
   - Changes in processes, including forms, contracts, software programs, etc., since the previous examination.
   - Significant changes in policies, personnel, or controls.
   - Internal or external factors that could affect compliance with COPPA.
   - Whether applicable provisions of state laws and regulations are monitored and included in the bank's audit.

6. Complete the "Quality of Risk Management" procedures.

7. Complete appropriate sections of the "Quantity of Risk" procedures. The procedures performed in the "Quantity of Risk" section should address areas of concern identified during the review of "Quality of Risk Management."

8. Complete the "Conclusion Procedures."

Quality of Risk Management

Conclusion: The quality of risk management is (strong, satisfactory, weak).

Policy

Conclusion: The board (has/has not) established appropriate policies to ensure compliance with the Children's Online Privacy Protect Act.

Objective: Determine whether the bank has appropriate formal/informal policies to ensure compliance with COPPA.

1. Determine whether the board has adopted, and management has implemented adequate policies and procedures to maintain compliance with COPPA. Where appropriate, they should address:

   - Significant requirements of the law and the regulation.
   - Responsibilities and accountabilities of key personnel.
   - Training program.
   - Process for responding to changes in the law and the regulation.
   - Role of audit and compliance review.

2. Determine whether the board or an appropriate committee periodically reviews and approves compliance policies.

Processes

Conclusion: Management (has/has not) established effective processes to ensure compliance with COPPA.

Objective: Determine the reliance that can be placed on the bank's processes to prevent violations of COPPA.

1. Determine whether the bank's system for communicating the requirements of, and any subsequent changes to, COPPA is adequate to ensure ongoing compliance.

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

- Organization chart to determine who is responsible for the institution's compliance with COPPA;
- Process flow charts 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 Web site or online service;
- List of data elements collected from a child and a description of how the data are used and protected;
- List of data elements collected from a child that are disclosed to third parties and any contracts or agreements governing the use of that information with those third parties;
- Internal checklists, worksheets, and other review documents.

3. Assess the procedures used to ensure compliance when new online products are developed and operational changes are made.

Personnel

Conclusion: Bank management and personnel (do/do not) possess the required technical skills and knowledge to ensure compliance with COPPA.

Objective: Determine whether bank management and personnel possess sufficient knowledge and technical skills to manage and perform duties related to COPPA.

1. Assess bank management and personnel's knowledge and technical skills regarding COPPA based on conclusions developed while performing these procedures. Also consider:
   - Employee roles and responsibilities.
   - Training and experience.
   - Violations cited.
2. Review the bank's training program (materials, agendas, rosters, frequency, evaluation forms, etc.) and discuss with management to

determine how frequently and how well employees are trained regarding compliance with COPPA.

Controls

Conclusion: Management (has/has not) established effective control systems to ensure compliance with COPPA.

Objective: Determine the reliance that can be placed on the bank's control systems to detect and correct violations of COPPA, including practices and procedures performed by audit and compliance review.

1. Review audit and compliance review material, including working papers and reports, to determine whether:

   - The procedures address the COPPA provisions applicable to the institution;
   - The audits and reviews performed were reasonable and accurate;
   - The frequency of the compliance review is satisfactory;
   - Effective corrective action occurred in response to previously identified deficiencies; and
   - Deficiencies, their causes, and the effective corrective actions are consistently reported to management or the members of the board of directors.

2. Review the following documents and discuss with management to determine whether management information systems are sufficient and whether adequate practices are in place to ensure that timely and appropriate corrective action is taken when weaknesses/violations are identified or when consumer complaints indicate significant deficiencies.

   - Audit/compliance review policies, procedures, and work papers.
   - Audit/compliance review reports and management responses.
   - Management reports.

Quantity of Risk Management

Conclusion: The quantity of risk is (low, moderate, high).

Perform only those procedures identified as areas of concern during the review of the "Quality of Risk Management."

Objective: Determine the bank's level of compliance with COPPA.

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

   - Data are collected, used and shared in accordance with the institution's Web site notice [16 CFR 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 [16 CFR 312.5(a)].

2. Through discussions with management and a review of policies and procedures, determine whether the 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].

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

4. Through testing or management's demonstration of the Web site or online service, verify that the financial institution does not condition 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 is reasonably necessary to participate in the activity [16 CFR 312.7].

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

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

- Complies with a parent's instructions concerning the collection, use, maintenance, or disclosure of his or her child's information. [16 CFR 312.6(a)(2) and 16 CFR 312.4(b)(2)(iv) and (vi)];

- Allows a parent to review any personal information collected from his or her child [16 CFR 312.6(a)(3)]; and

- Verifies that the person requesting information is a parent of the child [16 CFR 312.6 (a)(3)].

6. Complete the "COPPA Worksheet For Notices" by reviewing notices on the Web site or online service.

Conclusions

Objective: Prepare written conclusion summaries, discuss findings with the EIC, and communicate findings to management. If necessary, initiate corrective action when policies or internal controls are deficient or when violations of law or regulation are identified.

1. Summarize findings and violations from the preceding procedural steps to assess the bank's level of compliance with COPPA.

2. For those violations found to be significant or a pattern or practice, determine the root cause of violation(s) by identifying weaknesses in:

   - Internal controls.
   - Audit/independent compliance review.
   - Training.
   - Management oversight.

3. Determine whether a civil money penalty (CMP) or an enforcement action should be recommended (refer to the CMP matrix).

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

5. Form a conclusion about the reliability of the compliance management system for COPPA and provide conclusions to the examiner performing the Compliance Management System program.

6. Determine whether any items identified during this examination could materialize into supervisory concerns before the next on-site examination (considering whether the bank has plans to increase monitoring in the affected area, or anticipates changes in personnel, policy, outside auditors or consultants, or business strategy). If so, summarize your concerns and assess the potential risk to the bank.

7. Determine the impact on the aggregate quantity and direction of risk assessment for any concerns identified during the review. Examiners should refer to guidance provided under the OCC's large and community bank risk assessment programs.

   - Risk categories: compliance, transaction, and reputation risk.
   - Risk conclusions: high, moderate, or low.

- Risk direction: increasing, stable, or declining.

8. Provide, and discuss with, the EIC (and the supervisory office, if appropriate) conclusions, including:

   - A summary of violations and recommended CMPs/enforcement actions, if any.
   - Potential reimbursements.
   - Recommended corrective action.
   - The quantity of risk and quality of risk management.
   - Recommended matters requiring attention (MRA). MRA should cover practices that:
     – Deviate from sound fundamental principles and are likely to result in financial deterioration if not addressed.
     – Result in substantive noncompliance with laws.
   - MRA should discuss:
     – Causative factors contributing to the problem.
     – Consequences of inaction to the institution.
     – Management's commitment for corrective action.
     – The time frame and person(s) responsible for corrective action.

9. Discuss findings with management. Obtain commitment(s) for corrective action as needed. Include in the discussion:

   - The quality of risk management.
   - The quantity of risk (include a listing of all violations, as well as significant violations).
   - MRA(s).

10. As appropriate, prepare a brief comment for inclusion in the report of examination.

11. Prepare a memorandum summarizing work performed (e.g., sampling method used, internal control systems, scope of audit review, conclusions regarding audit, etc.) and update the work program with any information that will facilitate future examinations. Update the OCC database on all violations of law or regulation.

12. Organize and reference working papers in accordance with OCC guidance (PPM 5400-8).

Children's Online Privacy Protection Act Worksheet for Notices

Every "No" answer indicates a potential violation of the regulation or an internal control deficiency and must be fully explained in the work papers.

Web site Notice (16 CFR 312.4)	**Yes**	**No**
1. A Web site link is posted 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 Web site's information practices with regard to children, and is 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 [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 Web site [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 [16 CFR 312.4(b)(2)(iv)]: – 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; • 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 • That 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 – The notice states the procedures for doing so [16 CFR 312.4(b)(2)(vi)].		
4. The notice to a parent • States that the operator wishes to collect information from the child [16 CFR 312.4(c)(1)(i)(A)]. • Includes the information contained in the 16 CFR 312.4(b) Web site notice (see step 3 above) [16 CFR 312.4(c)(1)(i)]. • If 16 CFR 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 16 CFR 312.5(c)(3) and (4) apply.		

Children's Online Privacy Protection Act

Appendix B

Request Letter Enclosure

1. COPPA policies and procedures.

2. COPPA training materials.

3. COPPA compliance reports, audit reports, procedures, and management responses. Note: If the bank participates in an FTC-approved, self-regulatory program, provide a copy of the program and audit reports.

4. Complaints regarding the collection, sharing, or use of data from a child.

5. Copies of Web site notices since the last examination.

6. A list of data elements collected from a child and a description of how the data are used and protected.

7. A list of data elements collected from a child that are disclosed to third parties and any contracts or agreements governing the use of that information with those third parties.

8. A list of parental requests for personal information provided by their children.

9. A description of how parental permission is obtained and the method of verifying that the person providing consent is the child's parent.

Laws

15 USC 6501 et seq., Children's Online Privacy Protection Act

Regulations

16 CFR 312, Children's Online Privacy Protection Rule

OCC Issuances

Bulletin 2001-8, "Guidelines Establishing Standards for Safeguarding Customer Information," dated 02/05/01.

Bulletin 2001-26, "Privacy of Consumer Financial Information; 12 CFR 40," dated 05/25/01.

Bulletin 2001-31, Weblinking," dated 07/03/01.

Bulletin 2001-35, "Examination Procedures to Evaluate Compliance with Guidelines to Safeguard Customer Information," dated 07/18/01.

Advisory Letter 2001-08, "Authentication in an Electronic Banking Environment," dated 07/30/01.

Children's Online Privacy Protection Act

Table of Contents

Children's Online Privacy Protection Act

Introduction

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 that is collected from children through Web sites 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 Web site(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.

Financial institutions that do not currently operate a Web site or online service directed to children, or do not have actual knowledge that they are collecting or maintaining personal information from a child online, are not subject to COPPA and will not be subject to COPPA examinations by the Office of the Comptroller of the Currency (OCC). However, financial institutions are urged to review their Web sites and their online information collection practices to ensure that they do not inadvertently trigger the provisions of this Act.

Definitions

"Child", "Children": (an) individual(s) under the age of 13.

"Personal information": 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 Web site 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 to the parent and on the Web site 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 and have deleted the personal information collected from his or 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).

Notice on the Web Site

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

An operator of a Web site or online service directed to children must post a link to a notice of its information practices with regard to children on its home page and at each area on the site or service where it collects personal information from any child. 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.

These links must be placed in a clear and prominent location on the home page of the Web site 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 that requires visitors to scroll down the 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 child through the Web site or online service;

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

- The way the operator uses, or may use, the personal information;

- A statement of 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 there is a prohibition against requiring, 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 has a right to 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 child can be made. 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's wishes to collect personal information from the parent's child;

- The requirement of the parent's consent for the collection, use, and disclosure of the information; and

- The way(s) the parent can provide consent.

Internal Uses [16 CFR 312.5(b)]

Financial institutions that use the personal information solely for internal purposes 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.

Disclosure to Others [16 CFR 312.5(b)]

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 requires a more reliable method of consent. The method used to obtain verifiable parental consent must be reasonably calculated, in light of available technology, to ensure that the person providing the consent is the child's parent. Methods that satisfy this requirement include:

- Obtaining a signed consent form from a parent via postal mail or facsimile;

- Accepting and verifying a parent's credit card number;

- Taking a parent's call, through a toll-free telephone number staffed by trained personnel;

- Receiving a parent's e-mail, accompanied by a digital signature; and

- Receiving an e-mail from a parent that is accompanied by a personal identification number (PIN) or password obtained through one of the methods mentioned above.

Disclosures to Third Parties [16 CFR 312.5(a)]

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 [16 CFR 312.5(a)]

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 [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 period 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 to, on a one-time basis, 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 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 Web site or online service is required to provide to a parent a means by which he or she can obtain any personal information collected from his or her child by that operator. 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. These methods might include requiring a parent to use a credit card in connection with a transaction; having a parent call a toll-free number staffed by trained personnel; using a digital certificate that uses public key technology; or using e-mail accompanied by a PIN or password.

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 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 any child.

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 Web site or online service that complies with FTC-approved, self-regulatory guidelines will receive a "safe harbor" from the requirements of COPPA and the regulation.

To be approved by the FTC, self-regulatory guidelines must include a requirement that operators subject to the guidelines implement substantially similar requirements that provide the same or greater protections for a child as the FTC regulation (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.

General Procedures

Objective: Determine the scope of the Children's Online Privacy Protection Act (COPPA) examination.

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

   - Is directed to children; or
   - Knowingly collects or maintains personal information from children.

   If the institution does not currently operate a Web site directed to children or knowingly collect information about them, the institution is not subject to COPPA, and no further examination for COPPA is necessary.

2. If the institution is subject to COPPA, determine whether it is participating in an FTC-approved, self-regulatory program (see 16 CFR 312.10). If it is, obtain a copy of the program and supporting documentation, such as reviews or audits, that demonstrate the institution's compliance with the program. If, under the self-regulatory program, an independent assessment found the institution in compliance with COPPA, or no assessment has yet been made, no further examination for COPPA is necessary. If, however, the independent assessment found the institution not in compliance with COPPA and the institution has not taken appropriate corrective action, continue with the procedures below.

3. If the institution is subject to COPPA and is not participating in an FTC-approved, self-regulatory program, continue with the procedures below.

4. From the examiner assigned the Compliance Management System program, obtain and review the following information to identify any previous or emerging problems that require follow-up:

   - Historical examination findings.
   - Complaint information from the bank and the OCC's Customer Assistance Group (CAG), and any CAG analytical reports, regarding the inappropriate collection, sharing, or use of data from a child.
   - Significant findings from the compliance audit.
   - Work papers from the prior examination.

5. Determine the following through early discussions with management:

   - Management supervision of compliance with COPPA, including responsiveness to, and corrective measures resulting from, consumer complaint activity.
   - Changes in processes, including forms, contracts, software programs, etc., since the previous examination.
   - Significant changes in policies, personnel, or controls.
   - Internal or external factors that could affect compliance with COPPA.
   - Whether applicable provisions of state laws and regulations are monitored and included in the bank's audit.

6. Complete the "Quality of Risk Management" procedures.

7. Complete appropriate sections of the "Quantity of Risk" procedures. The procedures performed in the "Quantity of Risk" section should address areas of concern identified during the review of "Quality of Risk Management."

8. Complete the "Conclusion Procedures."

Quality of Risk Management

Conclusion: The quality of risk management is (strong, satisfactory, weak).

Policy

Conclusion: The board (has/has not) established appropriate policies to ensure compliance with the Children's Online Privacy Protect Act.

Objective: Determine whether the bank has appropriate formal/informal policies to ensure compliance with COPPA.

1. Determine whether the board has adopted, and management has implemented adequate policies and procedures to maintain compliance with COPPA. Where appropriate, they should address:

   - Significant requirements of the law and the regulation.
   - Responsibilities and accountabilities of key personnel.
   - Training program.
   - Process for responding to changes in the law and the regulation.
   - Role of audit and compliance review.

2. Determine whether the board or an appropriate committee periodically reviews and approves compliance policies.

Processes

Conclusion: Management (has/has not) established effective processes to ensure compliance with COPPA.

Objective: Determine the reliance that can be placed on the bank's processes to prevent violations of COPPA.

1. Determine whether the bank's system for communicating the requirements of, and any subsequent changes to, COPPA is adequate to ensure ongoing compliance.

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

- Organization chart to determine who is responsible for the institution's compliance with COPPA;
- Process flow charts 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 Web site or online service;
- List of data elements collected from a child and a description of how the data are used and protected;
- List of data elements collected from a child that are disclosed to third parties and any contracts or agreements governing the use of that information with those third parties;
- Internal checklists, worksheets, and other review documents.

3. Assess the procedures used to ensure compliance when new online products are developed and operational changes are made.

Personnel

Conclusion: Bank management and personnel (do/do not) possess the required technical skills and knowledge to ensure compliance with COPPA.

Objective: Determine whether bank management and personnel possess sufficient knowledge and technical skills to manage and perform duties related to COPPA.

1. Assess bank management and personnel's knowledge and technical skills regarding COPPA based on conclusions developed while performing these procedures. Also consider:
   - Employee roles and responsibilities.
   - Training and experience.
   - Violations cited.
2. Review the bank's training program (materials, agendas, rosters, frequency, evaluation forms, etc.) and discuss with management to

determine how frequently and how well employees are trained regarding compliance with COPPA.

Controls

Conclusion: Management (has/has not) established effective control systems to ensure compliance with COPPA.

Objective: Determine the reliance that can be placed on the bank's control systems to detect and correct violations of COPPA, including practices and procedures performed by audit and compliance review.

1. Review audit and compliance review material, including working papers and reports, to determine whether:

   - The procedures address the COPPA provisions applicable to the institution;
   - The audits and reviews performed were reasonable and accurate;
   - The frequency of the compliance review is satisfactory;
   - Effective corrective action occurred in response to previously identified deficiencies; and
   - Deficiencies, their causes, and the effective corrective actions are consistently reported to management or the members of the board of directors.

2. Review the following documents and discuss with management to determine whether management information systems are sufficient and whether adequate practices are in place to ensure that timely and appropriate corrective action is taken when weaknesses/violations are identified or when consumer complaints indicate significant deficiencies.

   - Audit/compliance review policies, procedures, and work papers.
   - Audit/compliance review reports and management responses.
   - Management reports.

Quantity of Risk Management

Conclusion: The quantity of risk is (low, moderate, high).

Perform only those procedures identified as areas of concern during the review of the "Quality of Risk Management."

Objective: Determine the bank's level of compliance with COPPA.

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

   - Data are collected, used and shared in accordance with the institution's Web site notice [16 CFR 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 [16 CFR 312.5(a)].

2. Through discussions with management and a review of policies and procedures, determine whether the 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].

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

4. Through testing or management's demonstration of the Web site or online service, verify that the financial institution does not condition 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 is reasonably necessary to participate in the activity [16 CFR 312.7].

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

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

- Complies with a parent's instructions concerning the collection, use, maintenance, or disclosure of his or her child's information. [16 CFR 312.6(a)(2) and 16 CFR 312.4(b)(2)(iv) and (vi)];

- Allows a parent to review any personal information collected from his or her child [16 CFR 312.6(a)(3)]; and

- Verifies that the person requesting information is a parent of the child [16 CFR 312.6 (a)(3)].

6. Complete the "COPPA Worksheet For Notices" by reviewing notices on the Web site or online service.

Conclusions

Objective: Prepare written conclusion summaries, discuss findings with the EIC, and communicate findings to management. If necessary, initiate corrective action when policies or internal controls are deficient or when violations of law or regulation are identified.

1. Summarize findings and violations from the preceding procedural steps to assess the bank's level of compliance with COPPA.

2. For those violations found to be significant or a pattern or practice, determine the root cause of violation(s) by identifying weaknesses in:

   - Internal controls.
   - Audit/independent compliance review.
   - Training.
   - Management oversight.

3. Determine whether a civil money penalty (CMP) or an enforcement action should be recommended (refer to the CMP matrix).

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

5. Form a conclusion about the reliability of the compliance management system for COPPA and provide conclusions to the examiner performing the Compliance Management System program.

6. Determine whether any items identified during this examination could materialize into supervisory concerns before the next on-site examination (considering whether the bank has plans to increase monitoring in the affected area, or anticipates changes in personnel, policy, outside auditors or consultants, or business strategy). If so, summarize your concerns and assess the potential risk to the bank.

7. Determine the impact on the aggregate quantity and direction of risk assessment for any concerns identified during the review. Examiners should refer to guidance provided under the OCC's large and community bank risk assessment programs.

   - Risk categories: compliance, transaction, and reputation risk.
   - Risk conclusions: high, moderate, or low.

- Risk direction: increasing, stable, or declining.

8. Provide, and discuss with, the EIC (and the supervisory office, if appropriate) conclusions, including:

   - A summary of violations and recommended CMPs/enforcement actions, if any.
   - Potential reimbursements.
   - Recommended corrective action.
   - The quantity of risk and quality of risk management.
   - Recommended matters requiring attention (MRA). MRA should cover practices that:
     – Deviate from sound fundamental principles and are likely to result in financial deterioration if not addressed.
     – Result in substantive noncompliance with laws.
   - MRA should discuss:
     – Causative factors contributing to the problem.
     – Consequences of inaction to the institution.
     – Management's commitment for corrective action.
     – The time frame and person(s) responsible for corrective action.

9. Discuss findings with management. Obtain commitment(s) for corrective action as needed. Include in the discussion:

   - The quality of risk management.
   - The quantity of risk (include a listing of all violations, as well as significant violations).
   - MRA(s).

10. As appropriate, prepare a brief comment for inclusion in the report of examination.

11. Prepare a memorandum summarizing work performed (e.g., sampling method used, internal control systems, scope of audit review, conclusions regarding audit, etc.) and update the work program with any information that will facilitate future examinations. Update the OCC database on all violations of law or regulation.

12. Organize and reference working papers in accordance with OCC guidance (PPM 5400-8).

Children's Online Privacy Protection Act Worksheet for Notices

Every "No" answer indicates a potential violation of the regulation or an internal control deficiency and must be fully explained in the work papers.

Web site Notice (16 CFR 312.4)	**Yes**	**No**
1. A Web site link is posted 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 Web site's information practices with regard to children, and is 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 [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 Web site [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 [16 CFR 312.4(b)(2)(iv)]: – 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; • 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 • That 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 – The notice states the procedures for doing so [16 CFR 312.4(b)(2)(vi)].		
4. The notice to a parent • States that the operator wishes to collect information from the child [16 CFR 312.4(c)(1)(i)(A)]. • Includes the information contained in the 16 CFR 312.4(b) Web site notice (see step 3 above) [16 CFR 312.4(c)(1)(i)]. • If 16 CFR 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 16 CFR 312.5(c)(3) and (4) apply.		

Children's Online Privacy Protection Act

Appendix B

Request Letter Enclosure

1. COPPA policies and procedures.

2. COPPA training materials.

3. COPPA compliance reports, audit reports, procedures, and management responses. Note: If the bank participates in an FTC-approved, self-regulatory program, provide a copy of the program and audit reports.

4. Complaints regarding the collection, sharing, or use of data from a child.

5. Copies of Web site notices since the last examination.

6. A list of data elements collected from a child and a description of how the data are used and protected.

7. A list of data elements collected from a child that are disclosed to third parties and any contracts or agreements governing the use of that information with those third parties.

8. A list of parental requests for personal information provided by their children.

9. A description of how parental permission is obtained and the method of verifying that the person providing consent is the child's parent.

Laws

15 USC 6501 et seq., Children's Online Privacy Protection Act

Regulations

16 CFR 312, Children's Online Privacy Protection Rule

OCC Issuances

Bulletin 2001-8, "Guidelines Establishing Standards for Safeguarding Customer Information," dated 02/05/01.

Bulletin 2001-26, "Privacy of Consumer Financial Information; 12 CFR 40," dated 05/25/01.

Bulletin 2001-31, Weblinking," dated 07/03/01.

Bulletin 2001-35, "Examination Procedures to Evaluate Compliance with Guidelines to Safeguard Customer Information," dated 07/18/01.

Advisory Letter 2001-08, "Authentication in an Electronic Banking Environment," dated 07/30/01.