7. Any other factors the agencies determines to be relevant.

B. Compensation Leading to Material Financial Loss

Compensation that could lead to material financial loss to an institution is prohibited as an unsafe and unsound practice.

[60 FR 35678, 35682, July 10, 1995, as amended at 61 FR 43950, Aug. 27, 1996]

APPENDIX B TO PART 30—INTERAGENCY GUIDELINES ESTABLISHING INFORMATION SECURITY STANDARDS

TABLE OF CONTENTS

I. Introduction

The Interagency Guidelines Establishing Information Security Standards (Guidelines) set forth standards pursuant to section 39 of the Federal Deposit Insurance Act (section 39, codified at 12 U.S.C. 1831p–1), and sections 501 and 505(b), codified at 15 U.S.C. 6801 and 6805(b) of the Gramm-Leach Bliley Act. These Guidelines address standards for developing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information. These Guidelines also address standards with respect to the proper disposal of consumer information, pursuant to sections 621 and 628 of the Fair Credit Reporting Act (15 U.S.C. 1681s and 1681w).

A. *Scope*. The Guidelines apply to customer information maintained by or on behalf of entities over which the OCC has authority. Such entities, referred to as ''the bank,'' are national banks, federal branches and federal agencies of foreign banks, and any subsidiaries of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers). The Guidelines also apply to the proper disposal of consumer information by or on behalf of such entities.

B. *Preservation of Existing Authority*. Neither section 39 nor these Guidelines in any way limit the authority of the OCC to address unsafe or unsound practices, violations of law, unsafe or unsound conditions, or other practices. The OCC may take action under section 39 and these Guidelines independently of, in conjunction with, or in addition to, any other enforcement action available to the OCC.

C. *Definitions*. 1. Except as modified in the Guidelines, or unless the context otherwise requires, the terms used in these Guidelines have the same meanings as set forth in sections 3 and 39 of the Federal Deposit Insurance Act (12 U.S.C. 1813 and 1831p–1).

2. For purposes of the Guidelines, the following definitions apply:

a. *Board of directors*, in the case of a branch or agency of a foreign bank, means the managing official in charge of the branch or agency.

b. *Consumer information* means any record about an individual, whether in paper, electronic, or other form, that is a consumer report or is derived from a consumer report and that is maintained or otherwise possessed by or on behalf of the bank for a business purpose. Consumer information also means a compilation of such records. The term does not include any record that does not identify an individual.

i. *Examples*. (1) *Consumer information* includes:

(A) A consumer report that a bank obtains;

(B) Information from a consumer report that the bank obtains from its affiliate after the consumer has been given a notice and has elected not to opt out of that sharing;

(C) Information from a consumer report that the bank obtains about an individual who applies for but does not receive a loan, including any loan sought by an individual for a business purpose;

(D) Information from a consumer report that the bank obtains about an individual who guarantees a loan (including a loan to a business entity); or

(E) Information from a consumer report that the bank obtains about an employee or prospective employee.

(2) *Consumer information* does not include:

(A) Aggregate information, such as the mean credit score, derived from a group of consumer reports; or

(B) Blind data, such as payment history on accounts that are not personally identifiable, that may be used for developing credit scoring models or for other purposes.

c. *Consumer report* has the same meaning as set forth in the Fair Credit Reporting Act, 15 U.S.C. 1681a(d).

d. *Customer* means any customer of the bank as defined in §40.3(h) of this chapter.

e. *Customer information* means any record containing nonpublic personal information, as defined in §40.3(n) of this chapter, about a customer, whether in paper, electronic, or other form, that is maintained by or on behalf of the bank.

f. *Customer information systems* means any methods used to access, collect, store, use, transmit, protect, or dispose of customer information.

g. *Service provider* means any person or entity that maintains, processes, or otherwise is permitted access to customer information or consumer information through its provision of services directly to the bank.

II. STANDARDS FOR INFORMATION SECURITY

A. *Information Security Program.* Each bank shall implement a comprehensive written information security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the bank and the nature and scope of its activities. While all parts of the bank are not required to implement a uniform set of policies, all elements of the information security program must be coordinated.

B. *Objectives.* A bank's information security program shall be designed to:

1. Ensure the security and confidentiality of customer information;

2. Protect against any anticipated threats or hazards to the security or integrity of such information;

3. Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer; and

4. Ensure the proper disposal of customer information and consumer information.

III. DEVELOPMENT AND IMPLEMENTATION OF INFORMATION SECURITY PROGRAM

A. *Involve the Board of Directors.* The board of directors or an appropriate committee of the board of each bank shall:

1. Approve the bank's written information security program; and

2. Oversee the development, implementation, and maintenance of the bank's information security program, including assigning specific responsibility for its implementation and reviewing reports from management.

B. *Assess Risk.* Each bank shall:

1. Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems.

2. Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information.

3. Assess the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks.

C. *Manage and Control Risk.* Each bank shall:

1. Design its information security program to control the identified risks, commensurate with the sensitivity of the information as well as the complexity and scope of the bank's activities. Each bank must consider whether the following security measures are appropriate for the bank and, if so, adopt those measures the bank concludes are appropriate:

a. Access controls on customer information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing customer information to unauthorized individuals who may seek to obtain this information through fraudulent means.

b. Access restrictions at physical locations containing customer information, such as buildings, computer facilities, and records storage facilities to permit access only to authorized individuals;

c. Encryption of electronic customer information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access;

d. Procedures designed to ensure that customer information system modifications are consistent with the bank's information security program;

e. Dual control procedures, segregation of duties, and employee background checks for employees with responsibilities for or access to customer information;

f. Monitoring systems and procedures to detect actual and attempted attacks on or intrusions into customer information systems;

g. Response programs that specify actions to be taken when the bank suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies; and

h. Measures to protect against destruction, loss, or damage of customer information due to potential environmental hazards, such as fire and water damage or technological failures.

2. Train staff to implement the bank's information security program.

3. Regularly test the key controls, systems and procedures of the information security program. The frequency and nature of such tests should be determined by the bank's risk assessment. Tests should be conducted or reviewed by independent third parties or staff independent of those that develop or maintain the security programs.

4. Develop, implement, and maintain, as part of its information security program, appropriate measures to properly dispose of customer information and consumer information in accordance with each of the requirements of this paragraph III.

D. *Oversee Service Provider Arrangements.* Each bank shall:

1. Exercise appropriate due diligence in selecting its service providers;

2. Require its service providers by contract to implement appropriate measures designed to meet the objectives of these Guidelines; and

3. Where indicated by the bank's risk assessment, monitor its service providers to confirm that they have satisfied their obligations as required by section D.2. As part of this monitoring, a bank should review audits, summaries of test results, or other equivalent evaluations of its service providers.

E. *Adjust the Program.* Each bank shall monitor, evaluate, and adjust, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of its customer information, internal or external threats to information, and the bank's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to customer information systems.

F. *Report to the Board.* Each bank shall report to its board or an appropriate committee of the board at least annually. This report should describe the overall status of the information security program and the bank's compliance with these Guidelines. The reports should discuss material matters related to its program, addressing issues such as: risk assessment; risk management and control decisions; service provider arrangements; results of testing; security breaches or violations and management's responses; and recommendations for changes in the information security program.

G. *Implement the Standards.* 1. *Effective date.* Each bank must implement an information security program pursuant to these Guidelines by July 1, 2001.

2. *Two-year grandfathering of agreements with service providers.* Until July 1, 2003, a contract that a bank has entered into with a service provider to perform services for it or functions on its behalf satisfies the provisions of section III.D., even if the contract does not include a requirement that the servicer maintain the security and confidentiality of customer information, as long as the bank entered into the contract on or before March 5, 2001.

3. *Effective date for measures relating to the disposal of consumer information.* Each bank must satisfy these Guidelines with respect to the proper disposal of consumer information by July 1, 2005.

4. *Exception for existing agreements with service providers relating to the disposal of consumer information.* Notwithstanding the requirement in paragraph III.G.3., a bank's contracts with its service providers that have access to consumer information and that may dispose of consumer information, entered into before July 1, 2005, must comply with the provisions of the Guidelines relating to the proper disposal of consumer information by July 1, 2006.

SUPPLEMENT A TO APPENDIX B TO PART 30—INTERAGENCY GUIDANCE ON RESPONSE PROGRAMS FOR UNAUTHORIZED ACCESS TO CUSTOMER INFORMATION AND CUSTOMER NOTICE

I. BACKGROUND

This Guidance[1] interprets section 501(b) of the Gramm-Leach-Bliley Act (''GLBA'') and the Interagency Guidelines Establishing Information Security Standards (the ''Security Guidelines'')[2] and describes response programs, including customer notification procedures, that a financial institution should develop and implement to address unauthorized access to or use of customer information that could result in substantial harm or inconvenience to a customer. The scope of, and definitions of terms used in, this Guidance are identical to those of the Security Guidelines. For example, the term ''customer information'' is the same term used in the Security Guidelines, and means any record containing nonpublic personal information about a customer, whether in paper, electronic, or other form, maintained by or on behalf of the institution.

A. Interagency Security Guidelines

Section 501(b) of the GLBA required the Agencies to establish appropriate standards for financial institutions subject to their jurisdiction that include administrative, technical, and physical safeguards, to protect the security and confidentiality of customer information. Accordingly, the Agencies issued Security Guidelines requiring every financial institution to have an information security program designed to:

1. Ensure the security and confidentiality of customer information;

2. Protect against any anticipated threats or hazards to the security or integrity of such information; and

3. Protect against unauthorized access to or use of such information that could result

[1] This Guidance is being jointly issued by the Board of Governors of the Federal Reserve System (Board), the Federal Deposit Insurance Corporation (FDIC), the Office of the Comptroller of the Currency (OCC), and the Office of Thrift Supervision (OTS).

[2] 12 CFR part 30, app. B (OCC); 12 CFR part 208, app. D–2 and part 225, app. F (Board); 12 CFR part 364, app. B (FDIC); and 12 CFR part 570, app. B (OTS). The ''Interagency Guidelines Establishing Information Security Standards'' were formerly known as ''The Interagency Guidelines Establishing Standards for Safeguarding Customer Information.''

in substantial harm or inconvenience to any customer.

B. Risk Assessment and Controls

1. The Security Guidelines direct every financial institution to assess the following risks, among others, when developing its information security program:

a. Reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems;

b. The likelihood and potential damage of threats, taking into consideration the sensitivity of customer information; and

c. The sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks.[3]

2. Following the assessment of these risks, the Security Guidelines require a financial institution to design a program to address the identified risks. The particular security measures an institution should adopt will depend upon the risks presented by the complexity and scope of its business. At a minimum, the financial institution is required to consider the specific security measures enumerated in the Security Guidelines,[4] and adopt those that are appropriate for the institution, including:

a. Access controls on customer information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing customer information to unauthorized individuals who may seek to obtain this information through fraudulent means;

b. Background checks for employees with responsibilities for access to customer information; and

c. Response programs that specify actions to be taken when the financial institution suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies.[5]

C. Service Providers

The Security Guidelines direct every financial institution to require its service providers by contract to implement appropriate measures designed to protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer.[6]

II. RESPONSE PROGRAM

Millions of Americans, throughout the country, have been victims of identity theft.[7] Identity thieves misuse personal information they obtain from a number of sources, including financial institutions, to perpetrate identity theft. Therefore, financial institutions should take preventative measures to safeguard customer information against attempts to gain unauthorized access to the information. For example, financial institutions should place access controls on customer information systems and conduct background checks for employees who are authorized to access customer information.[8] However, every financial institution should also develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems[9] that occur nonetheless. A response program should be a key part of an institution's information security program.[10] The program should be appropriate to the size and complexity of the institution and the nature and scope of its activities.

In addition, each institution should be able to address incidents of unauthorized access

[3] *See* Security Guidelines, III.B.

[4] *See* Security Guidelines, III.C.

[5] *See* Security Guidelines, III.C.

[6] *See* Security Guidelines, II.B. and III.D. Further, the Agencies note that, in addition to contractual obligations to a financial institution, a service provider may be required to implement its own comprehensive information security program in accordance with the Safeguards Rule promulgated by the Federal Trade Commission (''FTC''), 16 CFR part 314.

[7] The FTC estimates that nearly 10 million Americans discovered they were victims of some form of identity theft in 2002. *See* The Federal Trade Commission, *Identity Theft Survey Report*, (September 2003), available at *http://www.ftc.gov/os/2003/09/synovatereport.pdf*.

[8] Institutions should also conduct background checks of employees to ensure that the institution does not violate 12 U.S.C. 1829, which prohibits an institution from hiring an individual convicted of certain criminal offenses or who is subject to a prohibition order under 12 U.S.C. 1818(e)(6).

[9] Under the Guidelines, an institution's *customer information systems* consist of all of the methods used to access, collect, store, use, transmit, protect, or dispose of customer information, including the systems maintained by its service providers. *See* Security Guidelines, I.C.2.d (I.C.2.c for OTS).

[10] *See* FFIEC Information Technology Examination Handbook, Information Security Booklet, Dec. 2002 available at *http://www.ffiec.gov/ffiecinfobase/html_pages/infosec_book_frame.htm*. Federal Reserve SR 97–32, Sound Practice Guidance for Information Security for Networks, Dec. 4, 1997; OCC Bulletin 2000–14, ''Infrastructure Threats—Intrusion Risks'' (May 15, 2000), for additional guidance on preventing, detecting, and responding to intrusions into financial institution computer systems.

to customer information in customer information systems maintained by its domestic and foreign service providers. Therefore, consistent with the obligations in the Guidelines that relate to these arrangements, and with existing guidance on this topic issued by the Agencies,[11] an institution's contract with its service provider should require the service provider to take appropriate actions to address incidents of unauthorized access to the financial institution's customer information, including notification to the institution as soon as possible of any such incident, to enable the institution to expeditiously implement its response program.

A. Components of a Response Program

1. At a minimum, an institution's response program should contain procedures for the following:

a. Assessing the nature and scope of an incident, and identifying what customer information systems and types of customer information have been accessed or misused;

b. Notifying its primary Federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of *sensitive* customer information, as defined below;

c. Consistent with the Agencies' Suspicious Activity Report (''SAR'') regulations,[12] notifying appropriate law enforcement authorities, in addition to filing a timely SAR in situations involving Federal criminal violations requiring immediate attention, such as when a reportable violation is ongoing;

d. Taking appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information, for example, by monitoring, freezing, or closing affected accounts, while preserving records and other evidence;[13] and

e. Notifying customers when warranted.

2. Where an incident of unauthorized access to customer information involves customer information systems maintained by an institution's service providers, it is the responsibility of the financial institution to notify the institution's customers and regulator. However, an institution may authorize or contract with its service provider to notify the institution's customers or regulator on its behalf.

III. CUSTOMER NOTICE

Financial institutions have an affirmative duty to protect their customers' information against unauthorized access or use. Notifying customers of a security incident involving the unauthorized access or use of the customer's information in accordance with the standard set forth below is a key part of that duty. Timely notification of customers is important to manage an institution's reputation risk. Effective notice also may reduce an institution's legal risk, assist in maintaining good customer relations, and enable the institution's customers to take steps to protect themselves against the consequences of identity theft. When customer notification is warranted, an institution may not forgo notifying its customers of an incident because the institution believes that it may be potentially embarrassed or inconvenienced by doing so.

A. Standard for Providing Notice

When a financial institution becomes aware of an incident of unauthorized access to sensitive customer information, the institution should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will

[11] *See* Federal Reserve SR Ltr. 00–04, Outsourcing of Information and Transaction Processing, Feb. 9, 2000; OCC Bulletin 2001–47, ''Third-Party Relationships Risk Management Principles,'' Nov. 1, 2001; FDIC FIL 68–99, Risk Assessment Tools and Practices for Information System Security, July 7, 1999; OTS Thrift Bulletin 82a, Third Party Arrangements, Sept. 1, 2004.

[12] An institution's obligation to file a SAR is set out in the Agencies' SAR regulations and Agency guidance. *See* 12 CFR 21.11 (national banks, Federal branches and agencies); 12 CFR 208.62 (State member banks); 12 CFR 211.5(k) (Edge and agreement corporations); 12 CFR 211.24(f) (uninsured State branches and agencies of foreign banks); 12 CFR 225.4(f) (bank holding companies and their nonbank subsidiaries); 12 CFR part 353 (State non-member banks); and 12 CFR 563.180 (savings associations). National banks must file SARs in connection with computer intrusions and other computer crimes. *See* OCC Bulletin 2000–14, ''Infrastructure Threats—Intrusion Risks'' (May 15, 2000); Advisory Letter 97–9, ''Reporting Computer Related Crimes'' (November 19, 1997) (general guidance still applicable though instructions for new SAR form published in 65 FR 1229, 1230 (January 7, 2000)). *See also* Federal Reserve SR 01–11, Identity Theft and Pretext Calling, Apr. 26, 2001; SR 97–28, Guidance Concerning Reporting of Computer Related Crimes by Financial Institutions, Nov. 6, 1997; FDIC FIL 48–2000, Suspicious Activity Reports, July 14, 2000; FIL 47–97, Preparation of Suspicious Activity Reports, May 6, 1997; OTS CEO Memorandum 139, Identity Theft and Pretext Calling, May 4, 2001; CEO Memorandum 126, New Suspicious Activity Report Form, July 5, 2000; *http://www.ots.treas.gov/BSA* (for the latest SAR form and filing instructions required by OTS as of July 1, 2003).

[13] *See* FFIEC Information Technology Examination Handbook, Information Security Booklet, Dec. 2002, pp. 68–74.

be misused. If the institution determines that misuse of its information about a customer has occurred or is reasonably possible, it should notify the affected customer as soon as possible. Customer notice may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the institution with a written request for the delay. However, the institution should notify its customers as soon as notification will no longer interfere with the investigation.

1. Sensitive Customer Information

Under the Guidelines, an institution must protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer. Substantial harm or inconvenience is most likely to result from improper access to *sensitive customer information* because this type of information is most likely to be misused, as in the commission of identity theft. For purposes of this Guidance, *sensitive customer information* means a customer's name, address, or telephone number, in conjunction with the customer's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer's account. *Sensitive customer information* also includes any combination of components of customer information that would allow someone to log onto or access the customer's account, such as user name and password or password and account number.

2. Affected Customers

If a financial institution, based upon its investigation, can determine from its logs or other data precisely which customers' information has been improperly accessed, it may limit notification to those customers with regard to whom the institution determines that misuse of their information has occurred or is reasonably possible. However, there may be situations where the institution determines that a group of files has been accessed improperly, but is unable to identify which specific customers' information has been accessed. If the circumstances of the unauthorized access lead the institution to determine that misuse of the information is reasonably possible, it should notify all customers in the group.

B. Content of Customer Notice

1. Customer notice should be given in a clear and conspicuous manner. The notice should describe the incident in general terms and the type of customer information that was the subject of unauthorized access or use. It also should generally describe what the institution has done to protect the customers' information from further unauthorized access. In addition, it should include a telephone number that customers can call for further information and assistance.[14] The notice also should remind customers of the need to remain vigilant over the next twelve to twenty-four months, and to promptly report incidents of suspected identity theft to the institution. The notice should include the following additional items, when appropriate:

a. A recommendation that the customer review account statements and immediately report any suspicious activity to the institution;

b. A description of fraud alerts and an explanation of how the customer may place a fraud alert in the customer's consumer reports to put the customer's creditors on notice that the customer may be a victim of fraud;

c. A recommendation that the customer periodically obtain credit reports from each nationwide credit reporting agency and have information relating to fraudulent transactions deleted;

d. An explanation of how the customer may obtain a credit report free of charge; and

e. Information about the availability of the FTC's online guidance regarding steps a consumer can take to protect against identity theft. The notice should encourage the customer to report any incidents of identity theft to the FTC, and should provide the FTC's Web site address and toll-free telephone number that customers may use to obtain the identity theft guidance and report suspected incidents of identity theft.[15]

2. The Agencies encourage financial institutions to notify the nationwide consumer reporting agencies prior to sending notices to a large number of customers that include contact information for the reporting agencies.

C. Delivery of Customer Notice

Customer notice should be delivered in any manner designed to ensure that a customer can reasonably be expected to receive it. For

[14] The institution should, therefore, ensure that it has reasonable policies and procedures in place, including trained personnel, to respond appropriately to customer inquiries and requests for assistance.

[15] Currently, the FTC Web site for the ID Theft brochure and the FTC Hotline phone number are *http://www.consumer.gov/idtheft* and 1–877–IDTHEFT. The institution may also refer customers to any materials developed pursuant to section 151(b) of the FACT Act (educational materials developed by the FTC to teach the public how to prevent identity theft).

example, the institution may choose to contact all customers affected by telephone or by mail, or by electronic mail for those customers for whom it has a valid e-mail address and who have agreed to receive communications electronically.

[66 FR 8633, Feb. 1, 2001, as amended at 69 FR 77616, Dec. 28, 2004; 70 FR 15751, 15753, Mar. 29, 2005; 71 FR 5780, Feb. 3, 2006]

APPENDIX C TO PART 30—OCC GUIDELINES ESTABLISHING STANDARDS FOR RESIDENTIAL MORTGAGE LENDING PRACTICES

TABLE OF CONTENTS

I. INTRODUCTION

i. These OCC Guidelines for Residential Mortgage Lending Practices (Guidelines) set forth standards pursuant to Section 39 of the Federal Deposit Insurance Act, 12 U.S.C. 1831p–1 (Section 39). The Guidelines are designed to protect against involvement by national banks and their operating subsidiaries, either directly or through loans that they purchase or make through intermediaries, in predatory or abusive residential mortgage lending practices that are injurious to bank customers and that expose the bank to credit, legal, compliance, reputation, and other risks. The Guidelines focus on the substance of activities and practices, not the creation of policies. The Guidelines are enforceable under Section 39 in accordance with the procedures prescribed by the regulations in 12 CFR part 30.

ii. As the OCC has previously indicated in guidance to national banks and in rulemaking proceedings (OCC Advisory Letters 2003–2 and 2003–3 (Feb. 21, 2003)), many of the abusive practices commonly associated with predatory mortgage lending, such as loan flipping and equity stripping, will involve conduct that likely violates the Federal Trade Commission Act's (FTC Act) prohibition against unfair or deceptive acts or practices. 15 U.S.C. 45. In addition, loans that involve violations of the FTC Act, or mortgage loans based predominantly on the foreclosure or liquidation value of the borrower's collateral without regard to the borrower's ability to repay the loan according to its terms, will involve violations of OCC regulations governing real estate lending activities, 12 CFR 34.3 (Lending Rules).

iii. In addition, national banks and their operating subsidiaries must comply with the requirements and Guidelines affecting appraisals of residential mortgage loans and appraiser independence. 12 CFR part 34, subpart C, and the Interagency Appraisal and Evaluation Guidelines (OCC Advisory Letter 2003–9 (October 28, 2003)). For example, engaging in a practice of influencing the independent judgment of an appraiser with respect to a valuation of real estate that is to be security for a residential mortgage loan would violate applicable standards.

iv. Targeting inappropriate credit products and unfair loan terms to certain borrowers also may entail conduct that violates the FTC Act, as well as the Equal Credit Opportunity Act (ECOA) and the Fair Housing Act (FHA). 15 U.S.C. 1691 *et seq.* 42 U.S.C. 3601 *et seq.* For example, ''steering'' a consumer to a loan with higher costs rather than to a comparable loan offered by the bank with lower costs for which the consumer could qualify, on a prohibited basis such as the borrower's race, national origin, age, gender, or marital status, would be unlawful.

v. OCC regulations also prohibit national banks and their operating subsidiaries from providing lump sum, single premium fees for debt cancellation contracts and debt suspension agreements in connection with residential mortgage loans. 12 CFR 37.3(c)(2). Some lending practices and loan terms, including financing single premium credit insurance and the use of mandatory arbitration clauses, also may significantly impair the eligibility of a residential mortgage loan for purchase in the secondary market.

vi. Finally, OCC regulations and supervisory guidance on fiduciary activities and asset management address the need for national banks to perform due diligence and exercise appropriate control with regard to trustee activities. See 12 CFR 9.6 (a) and Comptroller's Handbook on Asset Management. For example, national banks should exercise appropriate diligence to minimize potential reputation risks when they undertake to act as trustees in mortgage securitizations.

A. *Scope.* These Guidelines apply to the residential mortgage lending activities of national banks, federal branches and agencies