What you need to do now

I. Conduct an information inventory of each business unit and all delivery channels to assess existing information practices.

- You need to determine X
  - The personally identifiable information you **collect** about consumers.
  - The consumer information you **disclose** to third parties.
  - The **purpose** for disclosing consumer information.

II. Determine how your bank *wants* to handle/share customer information.

- The message you want to send to your customers about the privacy of their personal information.

A. If you are currently sharing information with third parties outside of the exceptions, ask yourself if X

1. The benefits of such sharing offset any increased compliance burden associated with the sharing.
2. Your customers will object to these sharing arrangements.

B. If you are not currently sharing information with third parties outside of the exceptions, ask yourself if X

1. Your business plans contemplate the sharing of information with third parties in the future.
2. Your privacy policy should reserve the right to share information with third parties in the future.

III. Develop a privacy compliance program.

A. Establish the bank's policies and practices to protect the **confidentiality and security** of consumer information, including consumer information that is disclosed to third parties.

B. Draft a **privacy policy**, or revise an existing policy, to reflect accurately your information handling practices and meet the regulatory requirements.

C. If you share information with nonaffiliated third parties outside of the exceptions, develop an **opt out** notice and a means to honor the wishes of consumers who choose to opt out of certain information sharing.

D. Establish **methods to deliver** your privacy policies to your customers.

E. Establish a **training program** for your employees.

F. Plan to **monitor, review, and revise** implementation of your compliance program to cover policy changes, information security issues, and employee training.

** Attached is a checklist of specific tasks intended to assist banks in complying with the requirements of the privacy regulations.*

Checklist of specific tasks to assist you in complying with the privacy regulations

I. Conduct an information inventory of each business unit and all delivery channels to assess existing information practices.

A. Determine your **consumers** and thus those entitled to privacy protections under the regulations by establishing:

1. The identity of individuals who obtain financial products or services from you primarily for personal, family, or household use and who have an ongoing relationship with you B i.e., your "consumer" **customers**. *Those customers are entitled to privacy notices and an opportunity to opt out of certain information sharing arrangements that you may have with nonaffiliated third parties.*

2. Whether you offer financial products or services to individuals primarily for personal, family, or household use with whom you do not establish an ongoing relationship. For instance, do you have an ATM available to individuals, who are not your customers, or do you provide travelers' checks or cashiers' checks to noncustomers? *Those individuals are considered your **consumers** and are entitled to a notice of your privacy policy and an opportunity to opt out of information sharing, <u>only if</u> you engage in certain types of information sharing arrangements with nonaffiliated third parties.*

B. Establish the consumer information that you collect and maintain that is **nonpublic personal information.** The regulatory requirements for notice, opt out, and safeguarding information apply only to nonpublic personal information. Information considered nonpublic personal information should become apparent from responses to the following questions:

1. What **personally identifiable financial information** do you collect from:

a. Your consumers, such as information on their applications?
b. Your transactions with consumers, such as types of accounts
they have with you and account activity?
c. Other sources in connection with providing a financial product
or service to consumers, such as a consumer reporting agency?

2. What personally identifiable financial information do you collect is **publicly available** B i.e., you have a reasonable basis to believe that the information is made available lawfully to the general public from government records, widely distributed media, or its disclosure is required by law?

3. What lists, descriptions, or other groupings of your consumers do you maintain or generate? *Any list derived from nonpublic personal information is protected under the regulations, even if every piece of information on the list is publicly available. A list of your depositors' names and addresses is nonpublic personal information.*

4. Which lists, descriptions, or other groupings of your consumers contain only publicly available information and are derived using only publicly available information? *A list of your mortgage account holders' names and addresses is available publicly, if you do business in a jurisdiction that requires you to record mortgages.*

C. Determine the nonpublic personal information you are **disclosing** and **to which type of third party.**

1. Do you disclose, or plan to disclose, nonpublic personal information to **affiliates**?

    a. What types of nonpublic personal information do you disclose?
    b. To what types of affiliated companies do you disclose nonpublic personal information?

2. Do you disclose, or plan to disclose, nonpublic personal information to **nonaffiliated third parties**?

    a. What types of nonpublic personal information do you disclose to nonaffiliated third parties?
    b. To what types of nonaffiliated third parties do you disclose nonpublic personal information?

3. Do you disclose your customers' **account numbers** to nonaffiliated third parties? If so, is it for use in marketing?

    a. For marketing your own products or services?
    b. For marketing to a participant in a private label credit card program, an affinity, or similar program?
    c. Is the number encrypted, and if so, do you withhold the code to decrypt?
    d. Is your disclosure no longer permissible under the regulation?

D. Establish the **purpose** for the disclosure of nonpublic personal information to nonaffiliated third parties. Do you disclose information:

1. To service or process a financial product or service that a consumer has requested or authorized?

2. To maintain or service a consumer's account?

3. To third parties that perform services or functions on your behalf, such as marketing your products or services?

4. To other financial institutions under a joint marketing agreement?

5. To administer benefits or claims relating to consumer transactions?

6. In connection with billing, check clearing, or collecting amounts charged?

7. To protect against fraud?

8. To persons acting in a fiduciary or representative capacity for the consumer?

9. To a consumer reporting agency?

10. For any other purpose permitted under an exception?

11. For any purpose not permitted under an exception?

II. Determine how your bank *wants* to handle/share customer information.

A. If you are currently disclosing information to nonaffiliated third parties outside of the exceptions:

1. Determine whether the benefits of these disclosures outweigh the additional costs of compliance, such as:

a. A lengthier privacy notice.
b. The need to provide an opt out notice and opt out mechanism to customers.

c. The need to provide "noncustomer" consumers with a privacy notice and opt out, if you disclose their information.
d. The need to provide revised notices, if you change your information disclosure practices.

2. Assess how your customers will react to these disclosures.

B. If you are not currently disclosing information to nonaffiliated third parties outside of the exceptions:

1. Determine whether your business plans contemplate the sharing of information with third parties in the future.

2. Determine whether your privacy policy should reserve the right to share information with third parties in the future, so that you do not need to subsequently revise your policy.

III. Develop a Privacy Compliance Program

➢ **Maintain the confidentiality and security of consumer information.**

A. What are your policies and practices for protecting the **confidentiality and security** of customer information in accordance with the security guidelines issued by the banking agencies?

1. Have you conducted a **risk analysis** to 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. Based on your risk analysis, have you designed a **written information security program** to control the identified risks, considering the extent to which the following measures are needed:

a. Access controls, such as controls to authenticate and permit access to customer information systems to authorized persons only?
b. Access restrictions at physical locations, such as buildings and computer facilities, to permit access to authorized persons only?
c. Encryption?
d. Procedures to ensure that systems modifications are consistent with your security program?
e. Dual control procedures, segregation of duties, and employee background checks?
f. Monitoring systems and procedures to detect actual and attempted attacks?
g. Response programs specifying actions to be taken when the bank suspects unauthorized access?
h. Measures to protect against destruction, loss, or damage of information from potential environmental hazards, such as fire and water damage?

3. Has the **board of directors** or an appropriate committee of the board, approved your written information security program?

4. Do you have plans to **train staff** to implement your security program?

5. Do you have plans to **test regularly** the key controls, systems, and procedures?

B. What are your practices for protecting the confidentiality and security of customer information in the hands of **third parties**?

1. What arrangements, agreements, or contracts do you have with nonaffiliated third parties for disclosing nonpublic personal information?

2. Do contracts detail responsibilities for the use and protection of consumer information?

Note that for information sharing arrangements pursuant to ∍ 40.13 that you entered into <u>*after*</u> *July 1, 2000, you must have a written contract ensuring the confidential treatment of consumer information. (For contracts entered into prior to that date, you have until July 1, 2002 to come into compliance.) These agreements involve nonaffiliated third parties who (1) market your own products or services, (2) market products or services that are offered under a joint agreement between you and another financial institution, or (3) are other financial institutions with whom you have a written contract to jointly offer, sponsor, or endorse a financial product or service.*

Even when the privacy regulations do not specify the need for a confidentiality agreement, the banking agencies' security guidelines require that all contracts with third party service providers, entered into after 30 days from the date the final guidelines are published in the Federal Register, must have provisions addressing the security of customer information. (Contracts entered into before that date must come into compliance by July 1, 2003.)

3. Do you **oversee service provider arrangements** in accordance with the banking agencies' security guidelines by :

   a. Exercising **due diligence** in selecting your service providers?

   b. **Monitoring** your service providers to the degree indicated by your risk assessment?

- **Develop a privacy policy or revise an existing policy to reflect accurately your information practices and meet the regulatory requirements.**

  A. Do you have a privacy policy that makes all relevant disclosures?

1. If you are an institution **with no affiliates** and **disclose information to nonaffiliated third parties only under the exceptions in sections 40.14 and 40.15**, does your policy contain each of the following items:

a. Categories of information that you collect?
b. Your policies and procedures for safeguarding consumer information?
c. A statement that you make disclosures to nonaffiliated third parties only as permitted by law?

2. If you also **disclose information to third party service providers** to market your own products or services or to other financial institutions under a **joint marketing arrangement** under an **exception in section 40.13**, does your policy contain each of the following items:

a. Categories of information that you collect?
b. Categories of information that you disclose and the categories of third parties to whom you disclose information pursuant to a contract for marketing services or to jointly offer, sponsor, or endorse a financial product or service?
c. Your policies and procedures for safeguarding consumer information?
d. A statement that you make disclosures to other nonaffiliated third parties as permitted by law?

3. If you **disclose information to affiliates and to nonaffiliated third parties outside of the exceptions**, does your privacy policy contain each of the following:

a. Categories of information that you collect?
b. Categories of information that you disclose?
c. Categories of affiliates and nonaffiliated third parties to whom you disclose information outside of the exceptions?

d. Categories of information about your former customers that you disclose and the categories of affiliates and nonaffiliated third parties to whom you disclose information outside of the exceptions?
e. If you disclose information to a nonaffiliated third party under section 40.13 for marketing, a separate statement of the categories of information that you disclose and the categories of third parties with whom you have contracted?
f. An explanation of the consumer's right to opt out of the disclosure of information, including any method available to the consumer for opting out?
g. Any disclosure that you are making under the Fair Credit Reporting Act about the ability of a consumer to opt out of affiliate information sharing?
h. Your policies and practices for safeguarding information?
i. A statement that you make disclosures to other nonaffiliated third parties as permitted by law?

4. Will you provide consumers, who are not customers, with a **short form** initial notice in connection with an opt out notice?

B. Is the notice of your privacy policy presented in a **clear and conspicuous** manner?

1. Is your privacy notice **reasonably understandable** to consumers, because you use one or more of the following devices (or other comparable device):

a. Concise information?
b. Short explanatory sentences or bullet lists?
c. Definite, concrete, everyday words, and active voice?
d. Lack of multiple negatives, legal and highly technical terms, and imprecise explanations?

2. Is your privacy notice **designed to call attention to the nature and significance of the information** contained within the notice, because you use one or more of the following devices (or other comparable device):

a. Plain language headings?
b. Easily read typefaces and type sizes?
c. Wide margins and ample line spacing?
d. Boldface or italics of key words?
e. Distinctive type sizes, styles, and graphic devices when combining a privacy notice in a form with other information?

C. Does the policy reflect your **actual practices**?

D. Has your policy been reviewed by senior management and the board, the compliance officer, and legal counsel?

➢ **Establish mechanisms to permit consumers to opt out, *only if* you disclose information outside of the exceptions.**

A. Does your opt out mechanism meet all of the regulatory requirements?

1. Is the opt out mechanism reasonably convenient for consumers, because you use one of the following devices (or some other device):

a. A check-off box in a prominent position on a relevant form with the opt out notice?
b. A reply form with the opt out notice?
c. An electronic means for consumers to agree to the electronic delivery of notices?
d. A toll-free telephone number?

2. What period of time do you allot consumers to opt out before you initially share their information? Is the time period reasonable?

3. How do you provide for an opt out by consumers who hold a financial product or service jointly?

4. Do you allow partial opt outs?

B. How will you administer consumer opt out elections?

1. How will you document consumer opt out elections and any subsequent decisions to revoke an opt out?

2. How long does it take for you to process a consumer's request to opt out? Do you process the request as soon as reasonably practicable?

3. Do you have systems that can block or flag information that you may not disclose because a consumer has opted out?

C. How will you notify consumers about their rights to opt out?

1. Do you provide adequate notice of a consumer's right to opt out by addressing each of the following items:

a. Identifying the categories of nonpublic personal information that you disclose or reserve the right to disclose to nonaffiliated third parties (outside of the exceptions)?
b. Identifying the categories of nonaffiliated third parties to whom you disclose this information?
c. Stating that the consumer can opt out of that information disclosure?
d. Identifying the financial products or services that the consumer obtains from you to which the opt out would apply, such as whether the opt out applies to a particular account or the consumer's entire relationship with you?
e. Stating a reasonable means for consumers to opt out?

2. Will you provide the opt out notice as part of your initial and annual notice of your privacy policy or will you provide a separate opt out notice to your consumers?

3. If you provide a separate opt out notice, will you also provide a copy of your initial privacy policy with that notice?

D. If you provide consumer reporting information (such as information from applications or consumer reports) to affiliates, you should determine the application of the notice and opt out provisions of the Fair Credit Reporting Act to your activities.

- **Determine methods to deliver privacy notices.**

A. Will you deliver initial and annual privacy notices, including any revised notices, short form initial notices, and opt out notices, so that each consumer can reasonably be expected to receive **actual notice** by:

1. Hand delivering notices to consumers who conduct transactions in person?
2. Mailing the notices to the consumer's last known address separately or with other information?
3. Providing electronic notice for consumers who conduct transactions electronically and who agree to receive electronic notice?
    - How will you obtain your consumers' agreement for electronic delivery?

B. Will you ensure that your customers (not consumers) can **retain or subsequently access** your initial and annual notices and any revised privacy notices by:

1. Providing written notices through hand or mail delivery?
2. Making your current privacy notice or a link to your notice available on your web site for customers who conduct transactions electronically and agree to electronic notice?

C. Will you deliver privacy notices jointly on behalf of one or more of your affiliates or other financial institutions?

1. If so, does the notice identify the institutions on whose behalf you are sending the notice?
2. Is the notice accurate for each institution on whose behalf you are sending the notice?

D. How will you provide your privacy notices to joint account holders?

- **Establish a training program for your employees.**

A. Which employees do you plan to train?

1. Will you provide some level of training for all employees?
2. Do some employees, depending on their job responsibilities, require more specialized training?

B. Identify the persons who will conduct the training, its content, and its timing.

- **Monitor, review, and revise implementation of your compliance program to cover policy changes, information security issues, and employee training.**

A. If you want to disclose information to nonaffiliated third parties in a way that was not described accurately in your privacy notice, you must provide a revised notice and allow consumers a reasonable opportunity to opt out before making the disclosure.

B. Monitor state laws, because you may be subject to additional restrictions or requirements, if applicable state laws provide greater consumer protections than the federal requirements under the Gramm-Leach-Bliley Act.

HANDOUT C
3 PAGES

Privacy Preparedness and Supervision

OCC Telephone Seminar
February 13 and 14, 2001

I. What examiners will be looking for prior to July 1, 2001.

A. Senior management and the board of directors should take appropriate steps to prepare and ensure compliance by the July 1, 2001 deadline. (See OCC Advisory Letter 2001-2.)

B. Banks should perform self-assessments and be prepared to discuss the results with the OCC.

i. Attached to the Advisory is a privacy preparedness questionnaire that can be used to perform a privacy self-assessment.

ii. During the 2001 quarterly reviews of your bank, examiners will inquire about your privacy policies and preparations, and the results of any self-assessment.

iii. Examiners will use the questionnaire to ask applicable questions about your privacy readiness and may also offer suggestions to improve your compliance efforts.

II. What to expect from a privacy examination after July 1, 2001.

A. Risk-based Approach

i. Using the results of the quarterly reviews, the OCC will assess the level of risk at each bank as it relates to compliance with the privacy regulation.

ii. The level of risk will determine the scope and timing of future examinations.

a. High-risk banks will be examined within the 18-month period following July 1, 2001.

b. Banks with less risk will be reviewed during their next regularly scheduled compliance examination.

c. It is anticipated that all large- and mid-size banks will be examined within the 18-month period following July 1, 2001.

B. Privacy Examination Objectives

i. Assess the quality of the bank's compliance management policies and procedures for implementing the privacy regulation, specifically ensuring that the bank's privacy practices are consistent with its stated policies.

ii. Determine the reliance that can be placed on the bank's internal controls and procedures for monitoring compliance with the privacy regulation.

iii. Determine the bank's overall compliance with the privacy regulation.

iv. Initiate corrective actions when violations of law are identified, or when policies or internal controls are deficient.

C. Examination Procedures

i. Interagency product (FFIEC).

a. Still in the finalization stages.

ii. The level of risk associated with the bank's practices will dictate the transactional testing procedures to be performed.

iii. The level of risk will be determined by:

a. The bank's information sharing practices with affiliates, nonaffiliated third parties, and others.

b. The way the bank treats nonpublic personal information.

c. The way the bank administers opt-outs.

d. Consumer complaints about the treatment of nonpublic personal information.

e. The level of internal controls, including compliance audit and procedures in place to ensure compliance with the privacy regulation.

Office of the Comptroller of the Currency
Program Evaluation

This form is electronically tallied. Please mark only one circle for each question.
Do not mark outside the circles.

Privacy Regulation Compliance: February 13, 2001 OCC6059-1

Scale Definition: **P - Poor** **F - Fair** **G - Good** **VG - Very Good** **E - Excellent**

	P	F	G	VG	E
1. Overall rating of program	○	○	○	○	○
2. Similarity of actual program content to advertised content	○	○	○	○	○
3. Ease of registration	○	○	○	○	○
4. Audibility of seminar	○	○	○	○	○

Presenter: Overall Effectiveness

5. John D. Hawke, Jr.	○	○	○	○	○
6. Amy Friend	○	○	○	○	○
7. Mark Tenhundfeld	○	○	○	○	○
8. Ralph Sharpe	○	○	○	○	○
9. Dave Hammaker	○	○	○	○	○

Participant Information

10. How many people listened at your site?

○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ 6-10 ○ 11-15 ○ 16-20 ○ 21+

	Y	N
11. Would you participate in another virtual seminar?	○	○

What was your overall impression of the program and the virtual seminar format? What topics would be of interest to you in the future? Additional Comments?

Name of Participant (optional): ______________________________

PLEASE FAX COMPLETED FORM TO 1-800-472-5138

2C7