

PRIVACY OF CONSUMERS' FINANCIAL INFORMATION PART 10 EXAM PROCEDURES

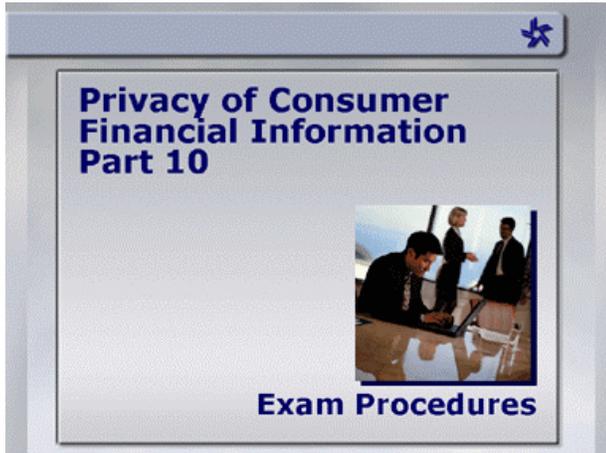
RESOURCES PROVIDED THROUGH

FFIEC InfoBase 

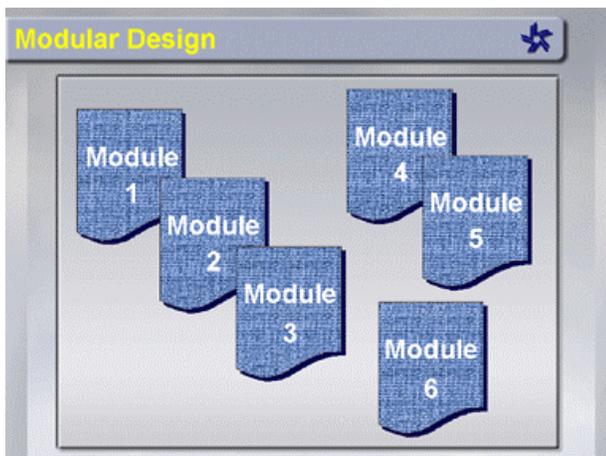
APRIL 2001

Slides

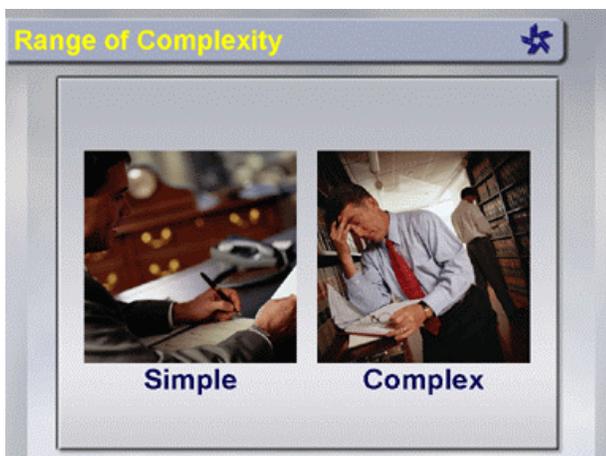
Narration



In this presentation, we're going to take a look at how the privacy exam procedures are organized. This overview will help you to discern more quickly the atypical way in which these particular procedures were designed.



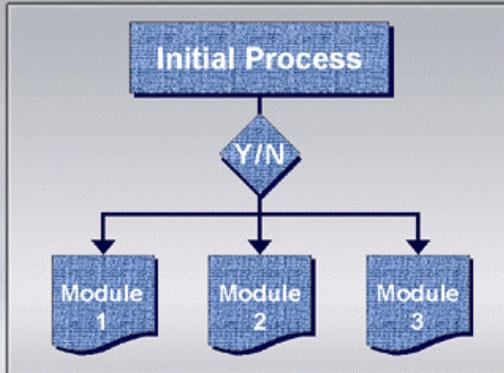
The exam procedures provide six different modules—designed to lead you through only those requirements applicable to the institution you're examining. The modules you use will depend on how the bank you are examining is handling privacy issues.



Some banks may not share any of their consumer's nonpublic personal information with nonaffiliated third parties—outside of the rule exceptions. Thus, these banks will need to meet only minimal requirements in order to comply with the privacy regulations.

On the other hand, banks may be engaged in multiple agreements with a variety of nonaffiliated third parties, necessitating a much more complex set of privacy notifications and internal operating procedures.

Notices and opt out



The exam process starts with a set of initial procedures to help you assess the scope of information sharing practices at the institution you are examining. You use the information gathered in the initial phase to work through a decision tree (also provided in the procedures) and to determine which modules are applicable to a particular exam.

You will select one of three possible modules for determining whether an institution’s privacy notices are accurate and that the bank has adequate procedures. The modules correspond with how an institution shares nonpublic personal information (about its consumers) with nonaffiliated third parties.

Exam Modules 1-3

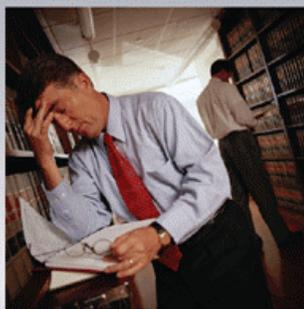
Privacy notices and opt out:

- ▶ Module 1
 - ▶ Sections 14 and/or 15
 - ▶ Opt out situations

Module one is for financial institutions that share nonpublic personal information with nonaffiliated third parties under:

- Sections 14 and/or Section 15 of the regulations (regardless of whether or not the institution is also sharing under Section 13) and under
- Situations outside of the exceptions (Situations that require an institution to provide an opportunity for customers to opt out of having their information shared).

Range of Complexity



Complex

Since these practices constitute the most expansive degree of information sharing that is permissible under the regulation, these institutions are also held to the most stringent compliance standards.

Exam Modules 1-3 

Privacy notices and opt out:

- ▶ **Module 1**
 - ▶ Sections 14 and/or 15
 - ▶ Opt out situations
- ▶ **Module 2**
 - ▶ Sections 13 and 14 and/or 15
 - ▶ Not outside of exceptions

Module two applies to financial institutions that share nonpublic personal information (with nonaffiliated third parties) under Sections 13, 14, and/or Section 15, but do not share information outside of exceptions in the regulations.

Exam Modules 1-3 

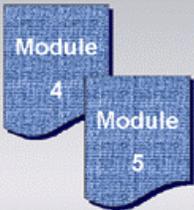
Privacy notices and opt out:

- ▶ **Module 1**
 - ▶ Sections 14 and/or 15
 - ▶ Opt out situations
- ▶ **Module 2**
 - ▶ Sections 13 and 14 and/or 15
 - ▶ Not outside of exceptions
- ▶ **Module 3**
 - ▶ Only Sections 14 and/or 15
 - ▶ Not outside of exception

Module three applies to financial institutions that share nonpublic personal information with nonaffiliated third parties only under Sections 14, and/or Section 15, but do not share information outside of those exceptions.

Reuse and Redisclosure 

▶ **How bank reuses/rediscloses information**

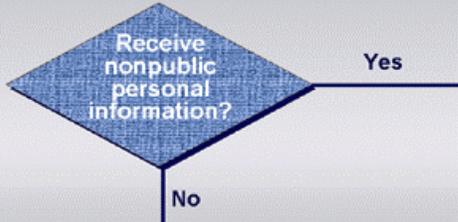


In addition to how a bank handles nonpublic personal information about its own consumers, you may also need to look at how the bank reuses and or rediscloses information it receives from other nonaffiliated financial institutions.

Let's take a look at how the decision tree process might work on this simple example.

Reuse and Redisclosure

▶ Does the institution being examined receive nonpublic personal information from any nonaffiliated financial institutions?



This time for determining which of two modules, if either, you should use to evaluate a particular bank.

The first question in the decision making tree is; "does the institution being examined receive nonpublic personal information from any nonaffiliated financial institutions?"

Decision Tree

▶ No – Review unnecessary

If a bank does not receive any nonpublic personal information from nonaffiliated financial institutions, obviously, you don't need to review this aspect of the bank's handling of privacy-related information.

Decision Tree

- ▶ No – Review unnecessary
- ▶ Yes
 - ▶ Under Sections 14 and/or 15
 - ▶ Outside of Sections 14 and 15

However, if the bank does receive such information,

Reuse and Redisclosure



- ▶ Under Sections 14 and/or 15 = Module 4

you will need to determine if it receives it under Sections 14 and/or 15 or outside of Sections 14 and 15.

Reuse and Redisclosure



- ▶ Under Sections 14 and/or 15 = Module 4
- ▶ Outside of Sections 14 and 15 = Module 5

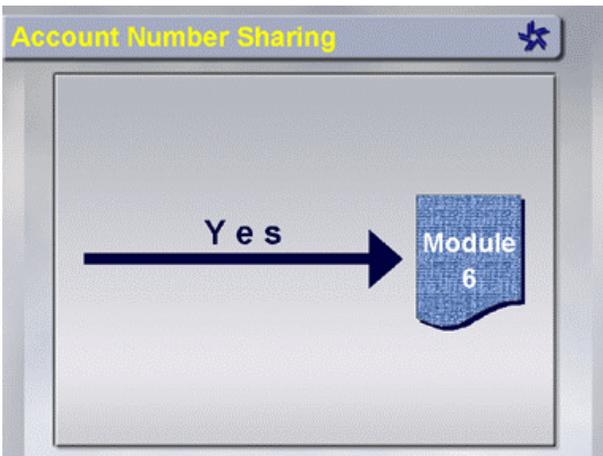
If the bank receives nonpublic personal information from a nonaffiliated third party under Sections 14 and/or 15 you will need to use module 4 of the procedures.

If the bank receives information outside of Sections 14 and 15 of rule, then you will need to use module 5 for your exam.

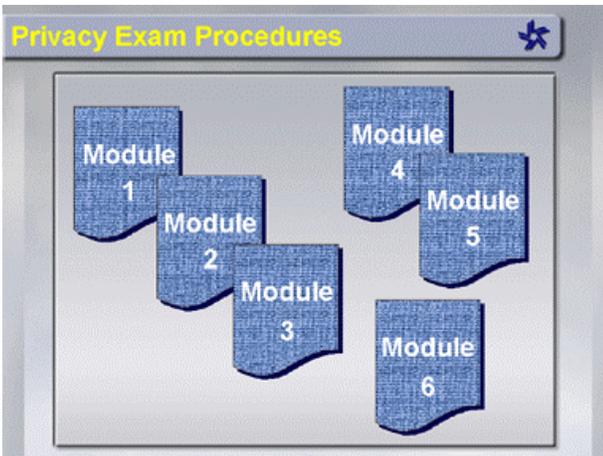
Account Number Sharing



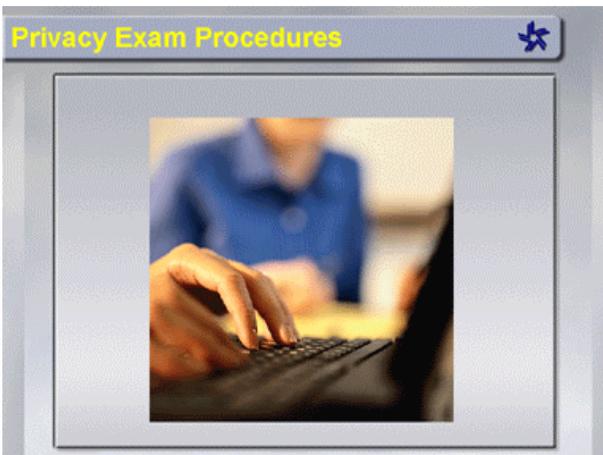
The sixth module in the procedures relates to a bank's sharing of consumers' account numbers or codes with nonaffiliated third parties (other than a consumer reporting agency) for telemarketing, direct mail, or electronic mail marketing.



If the bank does such sharing, you will need to use Module 6 of the exam procedures; if not, no review of this aspect of privacy is necessary.



That concludes our overview of the privacy exam procedures.



With this information, and that covered in earlier presentations, you should have a solid background for more detailed research and training in privacy requirements for consumer's financial information.

However, there's another topic that, although not related directly to compliance examinations, offers additional perspective on how banks should be responding to this emerging issue.

Section 501b



That topic is the requirements for the way in which a bank physically protects its consumer's nonpublic personal information—requirements set out in Section five O one b, of the G-L-B Act.

Section 501b



- ▶ Part 11 - 1501(b) Security Guidelines
- ▶ Part 12 - 501(b) and Bank Management

This issue is discussed in the last two presentations.