

## SAFEGUARDING CUSTOMER INFORMATION

W/P  
Reference

Comments

The following questionnaire may be used in assessing an institution's compliance with the Guidelines. Depending on the nature of the institution's operations and the extent of prior supervisory review, not all questions may need to be answered fully on each examination. Other examination resources may also be used if a technical evaluation of information security measures is needed. Examiners should conduct sufficient review in the following areas to provide a basis for evaluating the overall information security program and compliance with the Guidelines. See Federal Reserve SR Letter 01-15 "Standards for Safeguarding Customer Information," May 31, 2001, for further information.

1. Does the bank have a written information security program or policy? Has the written information security program been approved by the board of directors or an appropriate committee of the board?		
2. Is the written information security program appropriate given the size and complexity of the organization and its operations? Does it contain the objectives of the program, assign responsibility for implementation, and provide methods for compliance and enforcement?		
3. Does the bank periodically update its information security program to reflect changes in the bank's operations and systems, as well as changes in the threats or risks to the bank's customer information?		
4. Review the bank's process for assessing risk to its customer information. a) Has the bank identified the locations, systems, and methods for storing, processing, transmitting, and disposing of its customer information? b) Has the bank identified reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems and assessed the likelihood and potential damage to the bank and its customers of these threats?		
5. Review the bank's risk management processes for implementing effective		

	Initials	Date
Prepared by		

## SAFEGUARDING CUSTOMER INFORMATION

	W/P Reference	Comments
<p>measures to protect customer information. Does the bank consider the following areas, and adopt measures the bank concludes are appropriate based on risk?</p> <ul style="list-style-type: none"> <li>a) Access controls on computer systems containing customer information to prevent access by unauthorized staff or other individuals.</li> <li>b) Controls and procedures to prevent employees from providing customer information to unauthorized individuals, including "pretext calling."</li> <li>c) Access restrictions at physical locations containing customer information, such as buildings, computer facilities, and records storage facilities to permit access only to authorized individuals.</li> <li>d) The encryption of electronic customer information, including while in transit or in storage on networks or systems, in case unauthorized individuals are able to gain access.</li> <li>e) Procedures designed to ensure that modifications to customer information systems are consistent with the bank's information security program.</li> <li>f) Dual control procedures, segregation of duties, and employee background checks for employees with access to customer information to minimize risk of internal misuse of customer information.</li> <li>g) Monitoring systems and procedures to detect unauthorized access to customer information systems that could compromise the security of customer information.</li> <li>h) 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.</li> <li>i) 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.</li> </ul>		
<p>6. Have the bank's employees been trained to implement the information security program?</p>		
<p>7. Does the bank regularly test the</p>		

## SAFEGUARDING CUSTOMER INFORMATION

	W/P Reference	Comments
<p>effectiveness of key controls, systems, and procedures of its information security program? This may include, for example, tests of operational contingency plans, system security audits or “penetration” tests, and tests of critical internal controls over customer information. Are tests conducted by independent staff or are test results reviewed by independent staff?</p>		
<p>8. Does the bank provide customer information to any service providers or do any service providers have access to customer information through service provided directly to the bank?</p> <p style="margin-left: 20px;">a) If so, has the bank conducted appropriate due diligence in selecting its service providers, taking into consideration information security?</p> <p style="margin-left: 20px;">b) As of July 1, 2003, does the bank require its service providers by contract to implement appropriate information security programs and measures (or as of July 1, 2001 if contracts were entered into after March 5, 2001)?</p> <p style="margin-left: 20px;">c) Where appropriate based on risk, does the bank monitor its service providers to confirm that they are maintaining appropriate security measures to safeguard the bank’s customer information? For example, does the bank conduct or review the results of audits, security reviews or tests, or other evaluations?</p>		
<p>9. Does the bank report to its board or an appropriate committee of the board at least annually on the overall status of the information security program, including the bank’s compliance with the Guidelines and any other material matters?</p>		
<p><u>Conclusions</u></p> <p>10. Prepare a separate summary findings worksheet for this section of the work program. The summary shall include a</p>		

## SAFEGUARDING CUSTOMER INFORMATION

	W/P Reference	Comments
<p>discussion of the control strengths, weaknesses, deficiencies, or other problem and/or high-risk areas. Also include important facts, findings, examiner conclusions, and, if applicable, recommendations. Present conclusions about the overall condition of GLB compliance activities in this work program area.</p>		
<p>11. Discuss with management:</p> <ul style="list-style-type: none"> <li>a. Violations of law, rulings, regulations, or significant internal control deficiencies.</li> <li>b. Recommended corrective action for deficiencies cited.</li> <li>c. Management's proposed actions for correcting deficiencies.</li> <li>d. Reason(s) for not implementing a guideline or guidelines.</li> </ul>		
<p>12. Assign rating of Satisfactory, Needs Improvement, or Unsatisfactory.</p>		
<p>13. Prepare draft report comments for reportable findings and/or matters to be included in the administrative section of the ROE.</p>		
<p>14. Prepare an index of work papers for this section of the work program.</p>		
<p>15. Provide any additional information that will facilitate future examinations.</p>		