RESCINDED

OCC 1996-39

Subject: Data Communications Networks
Date: July 24, 1996

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

Description: Risks and Control Systems

OCC 1996-39 has been replaced by FFIEC Information Security Booklet.

appropriate measures should be taken to address any significant exposure to risk.

Background

National banks use data communications networks to provide access to their computer systems. These networks can consist of a mixture of different computer platforms (i.e., workstations, client servers, mini computers, mainframes, etc.) with a common network link. This allows users from various locations to communicate with each other and share information. Through "dial-in" capability, networks provide for the transmitting of information to and from bank customers and employees. Portions of these networks may be proprietary, while large public carriers may provide for other portions. More recently, networks have evolved that allow access to bank computer systems via the Internet.

The industry has developed various diagnostic tools such as network analyzers or "sniffers" to assist in troubleshooting and maintaining networks. While these tools serve legitimate business purposes, they can also be used by an unauthorized person to infiltrate a system to obtain critical information or sabotage computer systems. The sharing of information and resources through data communications networks increases the potential for unauthorized access and use, and therefore, poses additional risk to banks.

Risks AND CONTROL SYSTEMS

The risks associated with data communications networks can have a direct impact on a bank's earnings and capital. They primarily include transaction, strategic, and reputation risks.

These risks are directly related to a failure to properly perform or to deliver a quality product or service. Transaction risk generally arises from a breach or failure in controls or in the operation of systems that support such networks. Strategic risk arises from problems related to the design, development, and maintenance of a network's operating system. Reputation risk arises from the potential for adverse reaction in the marketplace due to unresolved problems and customer dissatisfaction associated with the delivery of a product or service through such networks. Bank management has the responsibility to maintain its awareness of these risks and to develop and implement reasonable control systems to manage them. Please refer to the Comptroller's Handbook Section on Bank Supervision Process for a detailed explanation of these risks.

Banks and data processing servicers have several controls they can use to reduce their vulnerability to risks associated with data communications networks especially those with "dial-in" access to a bank's computer systems. The objective of these controls is to assure that only authorized individuals enter these systems and, once the individuals gain access, those individuals can perform only authorized activities.

The level of controls placed on any given system or network should be commensurate with the bank's level of exposure and the cost of the control. Identifying and analyzing vulnerabilities as a part of an assessment of risks is an appropriate first step in managing these risks. Banks should consider outside sources if they do not have the in-house expertise to complete an assessment of the risks. Once this is complete, management should take appropriate measures to address any significant exposure. The primary objectives of these control systems should be to develop a high level of security discipline for the bank, its data processing servicers, and customers.

Controls for data communications networks should include the following:

- Developing and maintaining a methodology to govern passwords and user IDs.
- Identifying and authenticating individuals requesting access to the system and controlling their level of activity.
- Assuring, at the bank and customer level, that transactions are reconciled promptly.
- Ensuring the security of information during transmission across the network.
- Monitoring network use, including sign-on attempts, to identify anomalies.
- Developing and implementing appropriate firewalls to protect a "trusted" network from an "untrusted" network.

If a bank detects unusual activity on its data communications network, it may find it necessary to employ sophisticated techniques to identify its source. In the event the bank does not have resources appropriate for this task, they should consider engaging outside experts.

Please refer to the FFIEC Information Systems Handbook for a comprehensive discussion of controls over data communications networks.

Jimmy F. Barton
Chief National Bank Examiner