SCHWARTZ & BALLEN
1990 M STREET, N.W. · SUITE 500
Washington, DC 20036-3418

(202) 776-0700

FACSIMILE
(202) 776-0720

M E M O R A N D U M

December 11, 2000

To: **Our Clients and Friends**

Re: **Outsourced Technology Services**

Summary

The Federal Financial Institutions Examination Council (FFIEC) issued guidance on November 28, 2000 to financial institutions regarding the technology services supplied by outside service providers (the "SP"). Technology services covered by the FFIEC guidance include information and transactions processing, settlement, aggregation, digital certification and security monitoring to support banking functions. The FFIEC encourages financial institutions to consider further risk-management controls when outsourcing services involving the use of the internet.

The FFIEC expects the boards of directors and senior management of financial institutions to oversee and manage these outsourcing relationships. Financial institutions should implement an outsourcing process that includes: (1) a risk assessment to identify the institution's needs and requirements; (2) proper due diligence to identify and select a SP; (3) written contracts that clearly outline duties, obligations and responsibilities of the parties involved; and (4) ongoing oversight of outsourcing technology services. Each of these requirements is discussed below.

Risk Assessment

The risks involved in technology outsourcing include threats to security, availability and integrity of systems and resources, confidentiality of information and regulatory compliance. Also, credit, liquidity, transaction and reputation risks can result, depending on the nature of the transactions performed by the SP.

The board of directors and senior management are responsible for understanding the risks associated with outsourcing arrangements for technology services and ensuring that effective risk management practices are in place. Risk assessment should consider the following: strategic goals, objectives and business needs of the financial institution; ability to evaluate and oversee outsourcing relationships; importance of the services to the institution; defined requirements for the outsourced activity; necessary controls and reporting processes; contractual obligations for the SP; contingency plans; ongoing assessment of outsourcing arrangements; and regulatory requirements and guidance for the business lines affected and technologies used.

Due Diligence in Selecting a Service Provider

Once the institution has completed the risk assessment, management should evaluate the SPs to determine their operational and financial ability to meet the institution's needs. Factors for the institution to consider include the SP's technological and industry expertise (and identify where the institution would have to supplement the SP's expertise to fully manage risk), operations and controls (institution should look at the SP's security safeguards and internal controls), and the SP's financial condition. Institutions should also review the SP's own due diligence process in selecting subcontractors for these services.

Contract Issues

Financial institution management should consider certain issues when contracting with the SP. Appropriate legal counsel should review contracts prior to signing. If the SP cannot or will not agree to terms that the institution requests to manage risk effectively, the institution should not contract with the SP or should supplement the SP's commitments with additional risk mitigation controls. Contract issues include:

- Scope of Service. Management should consider: timeframes and activities for implementation and assignment of responsibility; services to be performed by the SP; obligations of the financial institution; contracting parties' rights to modify existing services performed under the contract; and guidelines for adding new or different services and for contract re-negotiation.

- Performance Standards. The contract should include standards defining minimum service level requirements and remedies for failure to meet these standards. The institution should periodically review overall performance standards as written in the contract are consistent with its goals and objectives.

- Security and Confidentiality. The contract should outline the SP's responsibility for security and confidentiality regarding the institution's resources (e.g., information, hardware). SP and its agents should be prohibited from using or disclosing the institution's information, except as necessary to provide the contracted services. If the SP receives nonpublic personal information regarding the institution's customers, the institution should notify the SP to assess the applicability of the privacy regulations. SP should be required to fully disclose breaches in security resulting in unauthorized intrusions into the SP that may affect the institution or its customers.

- Controls. The institution should consider to whom the contract gives control over operations, such as: internal controls to be maintained by the SP; compliance with regulatory requirements; records to be maintained by the SP; access to the records by the institution; notification by the SP to the institution and the latter's approval rights regarding material changes to services, systems, controls, key project personnel allocated to the institution, and new service locations; setting and monitoring parameters relating to any financial functions, such as payments processing and any extensions of credit on behalf of the institution; and insurance coverage to be maintained by the SP.

- Audit. The contract should include the types of audit reports the institution is entitled to receive (e.g., financial, internal control and security reviews). Management should consider (based on the risk assessment) the degree to which independent internal audits completed by SP audit staff can be used and the need for external audits and reviews. Where the services involve access to open networks, special attention should be paid to security. Periodic audits may be included in the contract terms, such as penetration testing, intrusion detection and firewall configuration.

- Reports. The contract should discuss the frequency and type of reports the institution will receive (e.g., performance reports, control audits, financial statements). Guidelines and fees for obtaining custom reports should be discussed as well.

- Business Resumption and Contingency Plans. The SP's responsibility regarding backup and record protection should be outlined in the contract. Responsibilities should include testing of the plans, and providing results to the institution. The institution should consider interdependencies among SPs when determining testing requirements. The SP should provide the institution with operating procedures to be implemented in the event business resumption contingency plans are implemented. Contracts should include business recovery timeframes that meet the

institution's business requirements, and the institution should ensure that the contract does not contain any provisions that excuse the SP from implementing its contingency plans.

- Sub-contracting and Multiple Service Provider Relationships. Where the SP contracts with a third party to provide services to the financial institution, it may be beneficial for the financial institution to include a provision specifying that the contracting SP is responsible for the service provided to the institution regardless of which entity is actually conducting the operations. The financial institution may also want to include notification and approval requirements regarding changes to the SP's significant subcontractors.

- Costs. The contract should fully describe all financial institution costs. The contract should include conditions under which the cost structure may be changed, as well as any limits on cost increases.

- Ownership and License. The contract should cover ownership and allowable use by the SP of the institution's data, equipment/hardware, system documentation, system and application software, and other intellectual property rights. Institutions that purchase software should consider establishing escrow agreements, which may provide for the following: institution access to source programs under certain conditions, such as insolvency of the vendor; documentation of programming and systems; and verification of updated source code.

- Duration of Relationship. This provision should consider the nature of the technology and state of the industry, in determining length of contract and renewal periods.

- Dispute Resolution. This provision should allow problems to be resolved expeditiously, while allowing a continuation of services during this process.

- Indemnification. The institution should take care to reduce the likelihood of instances where it is liable for the negligence of the SP.

- Limitation of Liability. The financial institution should consider whether any damage limitation bears an adequate relationship to the amount of loss the financial institution might reasonably experience as a result of the SP's failure to perform its obligations.

- Termination. The contract should allow the institution to terminate the arrangement in a timely manner without prohibitive expense. The contract should state

termination and notification requirements with time frames to allow the orderly conversion to another provider. The contract must provide for return of the institution's data and other resources in a timely manner.

- Assignment. The financial institution should consider whether the contract prohibits assignment of the contract to a third party without the financial institution's consent, including changes to subcontractors.

Oversight of Service Provider

Financial institutions should monitor the SP's performance, condition and controls throughout the relationship. Institutions are recommended to assess the quality of the SP's service and support; monitor contract compliance and revision needs; periodically monitor the SP's financial condition; review annual audit reports and insurance policies; and review the SP's business resumption contingency plans. Institutions should also take into consideration necessary oversight activities for any of the SP's subcontractors.

Please contact us if you have any further questions regarding the FFIEC guidance.