TB 59 was rescinded with the issuance of the FFIEC IT Examination Handbook's "Retail Payment Systems Booklet" (3/31/04) and "Outsourcing Technology Services Booklet" (7/15/04)

Handbook: EDP Examina
Subject: EFT Switches and Network Services

Section: 22
TB 59

May 19, 1993

RESCINDED

Interagency Supervisory Statement on EFT Switches and Network Services

Summary: The OTS has adopted an interagency supervisory statement on EFT Switches and Network Services.

For Further Information Contact: Your Regional Office, or Specialized Programs, Washington D.C.

Thrift Bulletin 59

This statement alerts the board of directors and senior management of financial institutions to the risks associated with switch and network services in retail electronic funds transfer (EFT) systems. Management of each institution that uses EFT switches and network services should implement policies consistent with this Bulletin.

Attachment

—John F. Robinson
Acting Deputy Director fo
Washington Operations

Federal Financial Institutions Examination Council

2100 Pennsylvania Avenue, NW, Suite 200 • Washington, DC 20037 • (202) 634-6526 • FAX (202) 634-6556

Interagency Supervisory Statement on EFT Switches and Network Services

To: Chief Executive Officers of all Federally Supervised Financial Institutions, Senior Management of each FFIEC Agency, and all Examining Personnel

PURPOSE

The purpose of this supervisory issuance is to alert the Board of Directors and senior management of financial institutions to the risks associated with switch and network services in retail electronic funds transfer (EFT) systems. This statement does not address wholesale or large dollar funds transfer systems such as FEDWIRE and CHIPS.

DEFINITIONS

A switch is a computer system that facilitates the transfer of electronic messages between terminal devices and the appropriate network participants. For example, it transmits an inquiry or transaction from an automated teller machine (ATM) or point-of-sale (POS) terminal to the depository institution that holds the customer's account. EFT terminals, processors, and switches can be configured in many different ways, depending on the participants' needs. The combination of interconnected terminals and computers is a network. Networks are sometimes operated by independent third party servicers.

BACKGROUND

Financial institutions have increased the use of switch and network services to lower costs and improve competitive position. Many financial institutions are sharing resources or using outside servicers, including non-financial companies, to provide EFT services. Such services include POS, ATM, and bill payment. Industry marketing efforts are promoting additional shared retail services, such as automated clearing houses (ACH), stored value cards, and credit card authorization.

EFT switches and network processing systems have expanded traditional methods of consumer banking, e.g., deposit, withdrawal, and obtaining credit. These systems provide customers with regional or nationwide access to their funds.

Some financial institutions are required by state law to share these services. Others voluntarily share them on a regional, national, or international basis.

Examples of shared EFT switch and network services include:

- o A multi-bank holding company network servicing affiliated institutions;
- o A network formed and shared by different types of financial institutions; and
- o A non-financial company's proprietary network shared with financial institutions for a fee.

Regardless of the types of services offered or systems being used, there are inherent risks in switch and network services.

CONCERNS

The increasing use of switches and networks raises certain concerns for participants:

- o OPERATIONAL FAILURE: System failure or service interruption, which may be caused by a disaster, could impact all connected financial institutions and could cause an erosion of consumer confidence;
- o SETTLEMENT FAILURE: Network participants could fail to make required settlement payment, resulting in significant financial losses; or, the processor could fail to provide necessary settlement records, forcing participants to reconstruct transactions;
- o FINANCIAL FAILURE: The switch servicer could experience sudden financial problems that may adversely impact all connected financial institutions;
- o DOLLAR LIMITS: The network's dollar limits, such as those applied to withdrawals, may be different from the limits the institution established;
- o AUDIT COVERAGE: Audits may not sufficiently cover internal controls, enforcement of standards, and review of transactions processed;
- o CONTRACTS: Poorly written contracts may inadequately define participants' liabilities and responsibilities and expose financial institutions to potential loss.

SUMMARY

The Board of Directors and senior management of financial institutions are responsible for:

- Ensuring that controls covering the switch processing environment are adequate. Alternatives to accomplish this objective include qualified internal or external auditors, or consultants specializing in this area. The results of these evaluations, and management's efforts toward correction, need to be documented in Board minutes.

- Ensuring that contracts for switches and network services are reviewed by legal counsel and meet minimum regulatory contract servicing guidelines. The guidelines are detailed in the FFIEC Interagency Statement on EDP Service Contracts (SP-6) and the FFIEC EDP Examination Handbook.

- Ensuring that settlement procedures do not pose undue risk to their institutions and that network rules adequately address actions that would be taken in the event that a participating institution fails to settle.

The appendix to this statement provides controls that should be in place in an EFT switch or network services environment.

APPENDIX

Control Objectives

Control for a safe and sound EFT network switching environment should address the following items. These objectives apply to all EFT switches and network servicers regardless of ownership:

Management:

- Written, approved, and enforced policies and procedures covering personnel, security controls, operations, and disaster recovery;
- Adequate segregation of duties and responsibilities;
- Periodic control evaluations of the switch and network;
- Daily settlement of switch activity and balancing of network activity, and periodic verification of fee distribution;
- Contracts that identify the responsibility and liability of all parties (e.g., timely presentment of returned items and appropriateness of fees and surcharges); and
- Adequate fidelity and business interruption insurance.

Security:

- Physical access restrictions;
- Encryption of critical data elements (e.g., personal identification code);
- Adequate management of encryption keys used in software;
- Software access controls including the program library, data files, and the network;
- Controlled access to positive and negative card files, used to authorize transactions; and institution control files (ICF) or institution parameter blocks (IPB), used to store institution-specific processing criteria; and
- Captured card procedures.

APPENDIX

Control Objectives (Continued)

Operations:

- o File backup and disaster planning including telecommunications;
- o Audit trails sufficient to trace transactions through the system;
- o Stand-in processing (having the cardholder data available at the switch for authorization) procedures should be available in the event of processor downtime, including the handling of positive balance files (PBF) and cardholder authorization systems (CAS);
- o Restart and recovery procedures to ensure the continuity of transaction processing in the appropriate sequence;
- o Controls over the embossing, encoding and distribution of access devices; and
- o Controls over the generation of cardholder personal identification codes (PIC) and communication of PICs to cardholders.