FEDERAL RESERVE BANK
OF DALLAS

ROBERT D. McTEER, JR.
PRESIDENT
AND CHIEF EXECUTIVE OFFICER

DALLAS, TEXAS
75265-5906

January 19, 1994

Notice 94-08

TO: The Chief Executive Officer of each member bank and others concerned in the Eleventh Federal Reserve District

SUBJECT

Control and Security Risks in Electronic Imaging Systems

DETAILS

The Federal Financial Institutions Examination Council's (FFIEC) Task Force on Supervision, acting under delegated authority, has adopted a supervisory issuance to alert senior management of each FFIEC Agency and all examining personnel to the risks associated with electronic imaging systems in financial institutions.

ATTACHMENT

A copy of the FFIEC's supervisory issuance is attached.

MORE INFORMATION

For more information, please contact Gary Krumm at (214) 922-6218 or Howard Edmonds at (214) 922-6278. For additional copies of this Bank's notice, please contact the Public Affairs Department at (214) 922-5254.

Sincerely yours,

Robert D. McTeer, Jr.

Federal Financial Institutions **Examination Council**

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

CONTROL AND SECURITY RISKS IN ELECTRONIC IMAGING SYSTEMS

TO: Senior Management of each FFIEC Agency and all Examining Personnel

PURPOSE

This issuance advises the senior management and examining personnel of each FFIEC agency of risks associated with electronic imaging systems in financial institutions.

DEFINITION

Electronic imaging systems is a term that describes the technology used to capture, index, store and retrieve electronic images of paper documents.

BACKGROUND

Technological advances in document scanning and optical character recognition are replacing the traditional paper storage systems in financial institutions. These systems incorporate new technologies such as optical disk storage, high resolution displays, document scanners, and laser printers to capture, store and print documents. Once stored in electronic form, the documents can be accessed throughout the organization. Image systems can range from small systems supporting a business function or department with a few users, to large systems or networks supporting multiple departments with hundreds of users.

Imaging systems replace the handling, distribution and storage of paper documents with electronic images. They are generally grouped into two types of systems: Document Management Systems and Item Processing Systems.

Document Management Systems

Document management imaging systems automate the flow of paper documents processed by departments and offices in a financial institution. These applications are referred to as "low-speed" imaging systems as documents contained in office or customer file folders are scanned one at a time. The process consists of

capturing original documents in electronic form on a low-speed scanning device, entering additional data and text into the record via keyboard entry, indexing the file folder and documents in a computer data base, and storing the folder on electronic storage media. Documents can then be displayed on a computer terminal, processed, or printed at work stations throughout the organization. These systems allow for the automatic routing of electronic documents to those individuals involved in the review or decision making process. They can also route documents or file folders for quality control reviews.

Document management systems account for the majority of imaging systems in financial institutions today. Examples of business functions where original documents (loan applications, customer correspondence, etc.) are being converted to imaging systems to improve processing and customer service are:

- o customer service account inquiries
- o student loan processing
- o loan/mortgage servicing applications
- o IRA/Keogh files
- o trust files
- o signature verifications
- o accounts payable

Item Processing Systems

Item processing imaging systems automate check or remittance processing applications on reader-sorters or similar high speed capture equipment. Images of transaction items are captured and stored for later use in encoding documents and exception processing. Item processing imaging systems require special attention to the quality and readability of the imaged documents. These high speed systems are relatively expensive to install as they require special scanning equipment, expanded storage capacity, and complex software programs to convert documents into readable electronic images.

Examples of item processing applications where transaction documents are converted to images for processing are:

- o proof-of-deposit
- o sales draft (credit card/POS) processing
- o remittance processing
- o account reconciliation processing
- o statement rendering

CONTROL AND SECURITY RISK AREAS

The replacement of paper documents with electronic images can have a significant impact on the way that an institution does business. Many of the traditional audit and security controls for paper based systems may be reduced or absent in electronic document workflow. New controls must be developed and designed into the automated process to ensure that information in image files cannot be altered, erased or lost.

Risk areas that management should address when installing imaging systems, and that examiners should be aware of when examining an institution's controls over imaging systems, are listed below:

Planning The lack of careful planning in selecting and converting paper systems to document imaging systems can result in excessive installation costs, the destruction of original documents, and the failure to achieve expected benefits. Critical issues such as converting existing paper storage files, integration of the imaging system into the organization workflow, and equipment backup and recovery procedures should be addressed to avoid reduced customer service and business interruptions.

Audit Imaging systems may change or eliminate the traditional controls, and checks and balances, inherent in paper based systems. Audit procedures may have to be redesigned, and new controls designed into the automated process. Audit departments should be sufficiently involved to ensure that electronic document work flows include appropriate audit controls and audit trails.

Redesign of Workflow Institutions generally redesign or reengineer workflow processes to benefit from imaging technology. New jobs or functions are identified and others eliminated. Changes may range from the redesign of forms to the reorganization of departments. Traditional controls such as time/date stamps, control numbers, review signatures, etc. may be replaced by limiting access to imaged documents, automated logs that report document access and retrieval information, etc. The absence of these, and other automated controls, may result in increased risks for the institution.

Scanning Devices Scanning devices are the entry point for image documents and a significant risk area in imaging systems. Scanning operations can disrupt workflow if the scanning equipment is not adequate to handle the volume of documents, or the equipment breaks down. The absence of controls over the scanning process can result in poor quality images, improper indexing, and incomplete or forged documents being entered into the system. Factors that should be considered in an imaging system are quality control over the scanning and indexing process, the scanning rate of the equipment, the storage of images, equipment backup, and the experience level of personnel performing the scanning function.

Indexing Poorly designed imaging system indexes can result in lost or inaccessible documents. Proper indexing of scanned documents is critical to later retrieval, and establishing access levels to individual documents and file folders. The integrity of indexes must be carefully maintained to ensure access to all documents and protection from unauthorized modification. The indexing method can affect the security administrator's ability to restrict access to documents or file folders. The institution should maintain automated journals and audit trails of document access and modifications to customer records.

Software Security Security controls over image system documents are critical to protect institution and customer information from unauthorized access and modifications. The integrity and reliability of the imaging system database is directly related to the quality of the controls over access to the system. Software

security and security administrator functions are essential to prevent unauthorized alterations to stored documents.

Contingency Planning and Backup Procedures Since more than 100,000 documents may be stored on a single optical disk, the loss of electronic image files or storage media can severely impact business operations if back-up electronic or paper files are not readily available. Contingency planning and back-up storage procedures for imaging system documents should follow generally accepted practices for data processing and management information systems.

Training Inadequate training of personnel scanning documents can result in poor quality document images and indexes, and the early destruction of original documents. The installation and use of imaging systems can be a major change for department personnel. They must be adequately trained to ensure quality control over the scanning and storage of imaged documents, as well as the use of the system to maximize the benefits of converting to imaging systems.

Legal Issues Case law on the admissibility of electronic image as evidence has not yet been established by the courts. Although precedent has been established on related electronic documents such as facsimile, microfilm, and photocopies, the courts have not addressed the authenticity of electronic images of original documents. Institutions installing imaging systems should carefully evaluate the legal implications of converting original documents to image, and the subsequent destruction of the original documents.

CONCLUSION

Imaging systems offer institutions benefits in streamlining department and office workflow processes, reduced storage and retrieval costs, and improved customer service by automating customer files and correspondence. These systems present new concerns and challenges for examiners and board of directors who must ensure that the risks are addressed by the institution's management.