

(FILE NAME ON DISK # 2 = S3C29.WPD)

TABLE OF CONTENTS

Number	Date	Subject
---------------	-------------	----------------

BANKING/OCC BULLETINS

OCC-94-8	01-27-94	Electronic Imaging Systems See FFIEC Policy SP-10 for details.
----------	----------	--

BANKING CIRCULARS

BC 177 Revised	07-12-89	Corporate Contingency Planning See FFIEC Policy SP-5 for details.
-------------------	----------	---

BC 187	01-18-85	Financial Information on Data Processing Servicers
--------	----------	---

BC 203 Revised	04-30-87	Accounting for the Cost of Internally Developed or Purchased Computer Software
-------------------	----------	---

BC 226	01-25-88	End-User Computing See FFIEC Policy SP-3 for details.
--------	----------	---

BC 229	05-31-88	Information Security
--------	----------	-----------------------------

BC 235	05-10-89	International Payments Systems Risks
--------	----------	---

BC 260	07-14-92	EDP Service Contracts See FFIEC Policy SP-6 for details.
--------	----------	--

BC 271	05-25-93	EFT Switches and Network Services See FFIEC Policy SP-9 for details.
--------	----------	--

EXAMINING CIRCULARS

EC 238 Supplement 1	08-02-89	Specialty Rating Disclosure
------------------------	----------	------------------------------------

EC-261	01-24-92	Interagency EDP Examination, Scheduling, and Report Distribution Policy See FFIEC Policy SP-1 for details.
--------	----------	--

OCC ADVISORY LETTERS

AL-88-7	11-21-88	Large-Scale Integrated Financial Software Systems
---------	----------	--

See FFIEC Policy SP-4 for details.

AL-91-4

07-24-91

Social Security Numbers as Personal Identification Numbers

Comptroller of the Currency Administrator of National Banks

OCC Bulletin 94-8
Date: January 27, 1994

Subject: Electronic Imaging Systems

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

Attached is a joint statement by the Federal Financial Institutions Examination Council on risks associated with electronic imaging systems. These systems are used to capture, index, store, and retrieve electronic images of paper documents. The statement discusses some potential risks to consider when planning for and using imaging technology.

Examiners will use the attached paper as a guideline when reviewing the operations of departments using imaging systems.

For further information, contact the Office of the Chief National Bank Examiner, (202) 874-5170.

/s/ Donald G. Coonley
Chief National Bank Examiner

Comptroller of the Currency Administrator of National Banks

**Banking Circular 177
(Revised)
Date: July 12, 1989**

Subject: Corporate Contingency Planning

To: Members of the Board of Directors of all National Banks, Chief Executive Officers of all National Banks, Deputy Comptrollers, District Administrators, and All Examining Personnel

PURPOSE:

Attached is a joint policy statement by the Federal Financial Institutions Examination Council (FFIEC). This policy addresses the need for corporate-wide contingency planning by all financial institutions and their servicers. This includes developing strategies to minimize loss and to recover from significant disruptions in business operations. At a minimum, these strategies must address:

- centralized and decentralized operations,
- user department activities,
- communications systems (data and voice),
- bank functions linked to service bureaus, and
- recovery plans by the service bureaus.

The attached policy statement revises Banking Circular 177, dated April 16, 1987. However, it reflects no change in policy by this Office toward contingency planning for national banks. It does represent a uniform policy by the FFIEC toward this important issue.

ORIGINATING OFFICE

Bank Information Systems Policy Division, (202) 447-0468

/s/ Robert J. Herrmann
Senior Deputy Comptroller for Bank Supervision

See FFIEC Policies SP-5 for details.

Comptroller of the Currency Administrator of National Banks

Banking Circular 187
Date: January 18, 1985

Subject: Financial Information on Data Processing Servicers

**To: Chief Executive Officers of All National Banks, District Deputy Comptrollers
and all Examining Personnel**

PURPOSE

The purpose of this Banking Circular is to alert national banks to the importance of performing financial reviews of organizations providing data processing services and to set forth OCC policy regarding the subject.

BACKGROUND

Financial institutions have become increasingly dependent upon computers for daily operations and must assure themselves of continued, uninterrupted data processing support. Many institutions use external (independent) data processors to provide such support.

Due to financial problems, several data processing servicers have failed and others have weakened, to the extent that their ability to continue operations and/or provide dependable services is uncertain. In many instances, the serviced financial institutions were unaware of the servicer's financial problems, and as a result, were unprepared for the data center's failure or the data center's inability to provide an acceptable level of service.

DISCUSSION

Financial institutions can reduce the potential impact of a data center failure by being informed of the financial condition of their servicers. Once aware of financial problems or an inability to provide an acceptable level of service, a financial institution could engage in alternative servicing arrangements and avoid an interruption in its data processing support. An effective method of obtaining financial information is to require, in the contracts between financial institutions and servicers, that current financial information be submitted on a regular basis.

POLICY

A board of Directors or a committee thereof in order to satisfy its fiduciary responsibilities regarding data processing services would normally obtain and analyze the financial information of their data processing servicers on an annual basis. Audited, unconsolidated financial statements would facilitate the analysis. If a servicer's financial condition is deteriorating or unsound, alternative

servicing arrangements should be considered in order to assure continued data processing support. Prudent banking practices would normally include the documentation of such analysis/contingency plans. For more information on Contingency Planning for Electronic Data Processing Support, See Banking Circular #177.

ORIGINATING OFFICE

EDP Examinations Division, (202) 447-0468

/s/ John F. Downey
Chief National Bank Examiner

Comptroller of the Currency Administrator of National Banks

**Banking Circular
203
(Revised)
Date: April 30, 1987**

Subject: Accounting for the Cost of Internally Developed or Purchased Computer Software

To: Chief Executive Officers of All National Banks, Deputy Comptrollers, District Administrators, Directors and Examining Personnel

PURPOSE

This issuance establishes a revised accounting policy for the cost of internally developed computer software consistent with generally accepted accounting principles.

REFERENCE

This Banking Circular supersedes the accounting policy previously established in Banking Circular No. 203, Accounting for the Cost of Internally Developed Computer Software. Banking Circular No. 203 is, therefore, rescinded.

POLICY

National banks should expense, as incurred, the cost of internally developed computer software developed for the bank's own use. This also includes the modification and implementation costs of purchased software.

Internally developed computer software which is intended to be sold, leased or otherwise marketed should be accounted for in accordance with Statement of Financial Accounting Standards No. 86 (FAS-86). "Accounting for the Costs of Computer Software to be Sold, Leased, or Otherwise Marketed." FAS-86 requires all such costs to be expensed as incurred until the software is determined to be technologically feasible. Thereafter, software production costs are to be capitalized and reported at the lower of unamortized cost or net realizable value. Amortization should be based on current and future revenues with the annual minimum amortization equal to the straightline amortization over the remaining estimated economic life of the product.

BACKGROUND

The Office of the Comptroller of the Currency (OCC) issued Banking Circular No. 203 because existing accounting literature provided only general guidance with respect to accounting for the cost of internally developed computer software. Further, this lack of specific guidance resulted in accounting policies which were not being consistently interpreted or applied.

Banking Circular No. 203 required all costs associated with internally developed computer software costs to be expensed as incurred. This policy applied both to software developed for the bank's own use, and to software intended to be sold, leased or otherwise marketed. When the Financial Accounting Standards Board later issued FAS-86, it varied with Banking Circular No. 203. This Circular revises the regulatory policy to be consistent with generally accepted accounting principles and FAS-86.

FAS-86 has excluded the costs incurred for an enterprise's development of computer software for its own use. This exclusion is based upon current accounting practice which heavily favors expensing such costs.

EFFECTIVE DATE

Costs incurred in the development of computer software for a bank's internal use must be expensed as of January 1, 1985. Retroactive application is encouraged.

Application of FAS-86 to costs incurred to develop computer software to be sold, leased or otherwise marketed is effective immediately. Retroactive application to the effective date set forth in FAS-86, fiscal years beginning after December 15, 1985, is allowed.

ORIGINATING OFFICE

Questions regarding this issuance may be directed to the Chief National Bank Examiner's Office. Bank Accounting Division (202) 447-0471.

/s/ William J. Stolte
Chief National Bank Examiner

Comptroller of the Currency Administrator of National Banks

**Banking Circular
226
Date: January 25,
1988**

Subject: End-User Computing

**To: Chief Executive Officers of All National Banks, Deputy Comptrollers, District
Administrators and All Examining Personnel**

PURPOSE

Attached is a joint issuance by the Federal Financial Institutions Examination Council on risks associated with end-user computing activities. End-user computing represents information processing activities which utilize microcomputers, small mainframes, and/or other computer terminals, to control and process data at the user level. It is recognized as a necessary and important aspect of information processing and delivery for many financial institutions.

This issuance discusses some of the potential risks and possible controls which are appropriate for these activities. Supervision and controls, consistent with guidelines offered in this circular, are expected for each national bank utilizing end-user computer systems.

ORIGINATING OFFICE

EDP Activities Division, (202) 447-0468

/s/ Robert J Herrmann
Senior Deputy Comptroller
for Bank Supervision

Attachment

See FFIEC Policies SP-3 for details.

Comptroller of the Currency Administrator of National Banks

Banking Circular 229
Date: May 31, 1988

Subject: Information Security

To: Chief Executive Officers of All National Banks, Deputy Comptrollers, District Administrators, and All Examining Personnel

PURPOSE

This circular alerts management of national banks to the importance of information security. It addresses the need to protect all types of information, particularly that which is produced, stored, and transmitted by computer.

BACKGROUND

Most bank information is created by or directly linked to computer processing. This includes customer records, financial transactions, business strategies, software systems, and even corporate correspondence. Financial data and business documents routinely are transmitted throughout a bank corporation via telecommunication lines linked to computers. Similar information also is transmitted outside the corporation, between the bank and its correspondents, its regulators, and its customers.

CONCERNS

Information, regardless of its source, is a valuable asset to the bank. Its accuracy and confidentiality is essential to the business. Accordingly, it must be protected from abuses such as inadvertent or intentional misuse, disclosure, fraud, and error. Information systems, both the data and the software that creates and stores the data, must be secure.

Data are created and stored in substantial volume, often representing millions of bank records and transactions. Correspondence and bank strategies also are created and stored through text processing. Bank and customer funds routinely are transferred via computerized payment networks. Transmission of these data regularly occur over public communications links, such as telephone lines and satellites. In addition, many users, including employees and bank customers, can directly access the data through computer terminals or telephones. Some have the ability to change information or create new data. These activities, while improving customer services and internal operations, also have increased the risk for error and abuse of the bank's information.

RECOMMENDATIONS

Controls must exist to minimize the vulnerability of all information and to provide necessary security. The level of control must be assessed against the degree of exposure and the impact of loss to the institution. This includes dollar loss, competitive disadvantage, damaged reputation, improper disclosure, lawsuit, or regulatory sanctions.

Various processes are available to strengthen information security in the banks. The most basic are sound written management policies for internal control. These include physical security, separation of duties, quality control, hardware and software access controls, and audit.

Information security controls should be designed to:

- ensure the integrity and accuracy of management information systems,
- prevent unauthorized alteration during data creation, transfer, and storage,
- maintain confidentiality,
- restrict physical access,
- authenticate user access,
- verify accuracy of processing during input and output,
- maintain backup and recovery capability,
- provide environmental protection against information damage or destruction.

Computer hardware and software technologies can help protect information resources. Although they vary, security features usually are available at each level of computer sophistication. Regardless of the controls adopted, they should apply to information produced and stored by both automated and manual methods.

The appendix to this issuance provides additional detail on some areas of risk and some technology controls. Additional control guidelines are detailed in the FFIEC EDP Examination Handbook.

POLICY

Information security is a functional responsibility. And as a means to protect assets, it must be a strategic objective of the business. A sound system of internal controls and management policies must be established and enforced to satisfy this objective.

The Board of Directors should require that information security policies exist throughout the bank corporation. These policies must be in writing and communicated to all personnel and other authorized users of bank information systems. Examiners may periodically target reviews of information security in the bank's supervisory strategy. These reviews may include:

- the adequacy of the "corporate information security policy,"
- compliance with the security standards, and
- management's supervision of these activities.

ORIGINATING OFFICE

Office of the Chief National Bank Examiner, Bank Information Systems Policy Division, (202) 447-0468

/s/ Donald G. Coonley
Chief National Bank Examiner
Attachment

BC-229 - Appendix

Banking Circular on Information Security

Some risk exists in every system and operation of the bank, whether manual or automated. Management must recognize the types of systems and operations that pose greater risks to information security. These might include:

- mainframe computer operations,
- microcomputer operations,
- communications networking,
- operating systems,
- applications software,
- end-user computing,
- distributed processing networks,
- system recovery activities,
- information retention and backup,
- text processing (office automation),
- document filing and retention,
- manual departmental operations.

Technology controls for information security might include:

Encryption

A process by which plain text is converted into encrypted strings of meaningless symbols and characters. This helps prevent unauthorized viewing and altering of electronic data transactions during transmission or storage. The Data Encryption Standard (DES) is commonly used for encoding PIN numbers on access cards, for storing user passwords, and for funds transfers on large dollar payment networks.

Message Authentication

A code (MAC) designed to protect against unauthorized alteration of electronic data transactions during transmission or storage. This code is used with data encryption to further secure transmission of large dollar payments.

Security Software

Application software designed to restrict access to computer-based data, files, programs, utilities, and system commands. Some systems can control access by user, by transaction, and by terminal. Security violations, including attempts can be reported. Access reports also can be produced.

Data Retention

The internal operations that require critical bank records to be regularly copied and stored in an offsite location. This includes data files, programs, operating systems, and related documentation. This also applies to critical data produced in hardcopy documents.

These are a few examples of controls and technologies to assist information security. New technologies and security methods are being developed and introduced constantly. The type and extent of controls must be measured against the degree of risk in any activity.

Comptroller of the Currency

Administrator of National Banks

Banking Circular 235

Date: May 10, 1989

Subject: International Payments Systems Risk

TO: Chief Executive Officers of All National Banks, Deputy Comptrollers, District Administrators, and All Examining Personnel

PURPOSE

To alert national banks to the risks associated with large dollar payments systems, particularly within the international sector, Management is expected to adopt sound policies and supervisory practices for these activities. This office recognizes that these risks are more prevalent in larger banks. However, all national bank participating in payments systems, domestic and international, must assess these risks.

ISSUE

The worldwide exchange of financial transactions and information is expanding rapidly. An interlocking network of national and international markets, operating 24 hours a day, supports this activity. This network involves multiple payments, clearing, and settlement systems that handle trillions of dollars daily. In recent years, attention by bankers and regulators has focused on the operational, liquidity, and credit risks of large dollar payments systems. However, this attention mainly addressed national systems such as FEDWIRE and the Clearing House for Interbank Payments (CHIPS). International payments, clearing, and settlement systems also demand a high level of supervision and risk assessment.

Key to each system is the credit quality of its participants and its operational reliability. These vary widely among systems and countries. A weakness in either or both of these attributes can disrupt the system and possibly cause it to fail. This may occur if a creditor in a given system cannot settle, if the support systems cannot operate, or if there is sovereign intervention. A failure in one system could pose a liquidity problem for participants in that system. If the liquidity risk is not contained, for example, through government guarantees or some participant allocation, the crisis can become systemic. The crisis can spread rapidly from participating banks to nonparticipants because of the interlocks between systems and banks.

The underlying risks remain the same for both national and international systems. However, the limited ability to influence policies and controls in international markets increases the degree of risk to national banks.

POLICY

Management of each national bank is responsible for assessing risk in each payments, clearing, and settlement system in which the bank participates. Management must adopt adequate policies, procedures, and controls with respect to these activities. At a minimum, written policies should:

-
- Require periodic risk assessment of each system in which the bank participates;
 - Identify responsibility for assessing risks;
 - Document procedures to perform the assessments;
 - Require top management approval of participation in selected system;
 - Establish a process to monitor on-going payments systems risk;
 - Require written agreements between the bank and both its customers and the network; and
 - Include audit in the review and compliance with these policies.

Additional detail on the risks in settlement systems is included in the Appendix to this circular.

Originating Office: Bank Information Systems Policy Division (202) 447-0468

/s/ Robert J. Herrmann
Senior Deputy Comptroller for
Bank Supervision - Policy

BC-235 - Appendix

Banking Circular on International Payments Systems Risk

The risks in payment systems may be divided into three broad categories:

- credit (or counterparty) risks,
- sovereign risks, and
- operational risks.

The control processes to assess risk and monitor on-going activities must consider payment systems as a whole. Although individual risks exist, they are interrelated. The effect of a single event creates additional risks within the system. For example, the effect of a single participant failing to meet its credit obligation may cause the system not to settle. As such, credit and settlement risk are interrelated. In another example, an operational breakdown in the system or sovereign action disrupts payments flow. The system, in turn, does not settle and credit obligations are not met. This example involves operations, settlement, and credit risk within the system.

Senior management must be both aware of and able to monitor exposure. Operating units of some banks are located throughout the world and may be participating in a number of payments systems. To control risk in these situations, some degree of centralized review is needed. This is particularly important in banks where local business units have significant autonomy. These banks may rely on local management to assess and manage the risks of participating in a network. Therefore, a bank's interdependency between systems also must be considered.

The control banks can exert over the systems in which they participate often is limited. A bank normally does not own or operate the systems. Bank management therefore must establish a process that assists them:

- Understanding the risks posed by participation in payment systems;
- Identifying bank policies designed to manage these risks; and
- Implementing procedures and operational controls to manage risk.

The following briefly identifies several control issues, types of settlement systems, and associated risks. These are not all encompassing. Much more detail is needed to perform a comprehensive risk assessment on any settlement system.

Other references include two recently published reports on this issue.

- 1) Report on Netting Schemes - February 1989
- prepared by the Group of Experts on Payment Systems of the Central Banks of the Group of Ten Countries
- 2) Clearance and Settlement Systems in the World's Securities Markets - March 1989
- prepared by the Group of Thirty

International Payments Systems Risk Appendix

CONTROL ISSUES

Management need to consider and resolve numerous issues when participating in payment systems. These issues are generally the same for both national and international systems.

Guidelines should consider:

- Controls to reduce sender and receiver risks. These should include:
 - Bilateral credit limits,
 - Debit cap limits, including the process to determine these limits.
 - A process to monitor and control these limits on a real time basis.
- Controls to limit the overall exposure of the system, including debit cap limits.
- Requirements of the system to ensure that settlement occurs. This should address:
 - conditions for settlement such as the location, time, and settling procedures.
 - the type of settlement (i.e., provisionality or finality of payment).
 - the guarantor(s), if any, of payment finality. This may involve a central bank, the system owner/operator, and/or the system participants.
 - the basis for providing necessary liquidity to the system. This may require allocation of funding by participants, coinsurance, or central bank guarantees.
- Legal issues governing the system operation, including local laws, business practices, and government regulation.
- The capabilities of the system and the bank to handle emergency situations. This may require backup operations or the ability for the bank to bypass the network.
- Responsibility for reviewing the bank's participation in payment systems.

SETTLEMENT SYSTEMS

NET SETTLEMENT SYSTEMS

Net settlement are systems in which transactions accumulate during a processing day. Transactions are posted to participant accounts on a provisional basis until final settlement. At end of the day, net debit positions pay, net credit positions settle, and all transactions become final. CHIPS is this type of system.

MATCHED SETTLEMENT SYSTEMS

Matched settlement systems are systems in which each transaction is "matched" by comparing messages from both counter parties to the transaction. Only exactly matched messages are allowed to enter the system to form a transaction. At the end of the processing day, the matched transactions become the basis for payment instructions issued to participants' clearing banks. Once payment is made, a transaction becomes final. CEDEL is this type of system.

International Payments
Systems Risk
Appendix
Page 3

GUARANTEE SETTLEMENT SYSTEMS

Guarantee settlement systems are systems in which payment finality is guaranteed by a central bank. Because payments are irrevocable, they eliminate risk to the receiver of funds. There is no credit risk to participants in such a system. However, the sovereign and operational risks may remain. A good example of this type of system is FEDWIRE, in which the Federal Reserve guarantees payment and finality. That system is still subject to potential risks from government action or operational failure.

SYSTEM RISKS

CREDIT RISKS

Sender Risk

Sender risk is the risk that a depository assumes when it makes an irrevocable payment on behalf of the customer through an extension of credit. Credit can be extended explicitly, by granting a loan, or implicitly, by paying against uncollected or provisional funds or against insufficient balances.

Receiver Risk

Receiver risk involves risk to an institution upon acceptance of funds from the sender. This may be a customer, another institution, or the payments system. As the receiver of funds, an institution must rely on the sender's ability to settle its obligations at the end of day. Receiver risk is present when payments are revocable within the system until final settlement.

SETTLEMENT RISKS

Settlement risk is the risk that each participant in the system will be able to honor all obligations at time of settlement. If one participant fails to settle, this may disrupt settlement for other participants. As a result, the system's settlement fails. This also is referred to as liquidity risk. Like receiver risk, settlement risk is present when payments are conditional or revocable until final settlement. Settlement risk also is an exposure subject to operational disruptions or sovereign actions.

NET SETTLEMENT SYSTEM RISKS

Net settlement systems bear all the risks identified above. However, an additional risk is that of default by the system itself. The system serves as a clearing mechanism for all transactions. At settlement, it posts a net debit or credit position to each participant's account. Each participant in a net debit position must provide funds to settle its position. If unable to settle, the system must cover the shortfall. If not, netted transactions unwind and other participants are affected.

International Payments
Systems Risk
Appendix
Page 4

The financial strength of the net settlement system itself, therefore, is a significant factor to assess. Often, this is provided through member pro rata guarantees or allocations. Also, the system's membership standards and operating procedures should ensure that the creditworthiness or operating practices of its members do not endanger the functioning of the system.

MATCHED SETTLEMENT SYSTEM RISKS

Credit risk in a matched settlement system should be addressed in the same way as for any bank customer. In matched systems the counterparty in a transaction is known to the bank and exposure to any one counterparty may be monitored and controlled through establishment of credit limits.

However, even in matched settlement systems attention should be given to the system's membership standards and operating procedures. The default of a participant may still impact a bank which has no settlements outstanding with it by the effect of the default on other participants with whom a bank does have understanding settlements.

SYSTEMIC RISKS

Systemic risk is an outgrowth of settlement risk. The failure of one participant to settle deprives other institutions of expected funds and prevents those institutions from settling in turn. To the extent that chains of obligations develop, it is possible for a participant doing no business at all with a failed institution to suffer because of the effect of the failed institution on an intermediate participant and its ability to settle.

LEGAL RISKS

Any transaction occurring in a payments system is subject to the interpretation of courts in different countries and legal systems. This issue is normally addressed by the adoption of "governing law" provisions in the rules of the systems themselves. These provide for all disputes between members to be settled under the laws of a specific jurisdiction. However, they may be of limited value if a local court refuses to recognize the jurisdiction of a foreign court. This risk is difficult to address because there is no binding system of international commercial law for electronic payments. Banks should seek legal opinions regarding the enforceability of transactions settled through a particular system.

SOVEREIGN RISKS

Sovereign risk applies to all types of payments systems. It is the risk that action by a government may affect either a system or particular participants in a system. This action could be detrimental to other participants in the system. An example of this risk would be the imposition of exchange control regulations on a bank participating in international foreign exchange activities. While the bank itself may be both willing and able to settle its positions, government intervention prevents it from doing so. This risk can be controlled by monitoring a bank's exposure to counter parties located in nations where this type of action is considered possible.

**International Payments
Systems Risk
Appendix
Page 5**

OPERATIONAL RISKS

Operational risks include:

- a) system failure - caused by a breakdown in the hardware and/or software supporting the system. This may result from design defects, insufficient system capacity to handle transaction volumes, or mechanical breakdown, including telecommunications.
- b) system disruption - the system is unavailable to process transaction. This may be caused by system failure, destruction of the facility (natural disasters, fires, terrorism) or operation shutdown (employee actions, business failure, or government action).
- c) system compromise - resulting from fraud, malicious damage to data, or error.

The loss of availability of the payment system from whatever source can adversely affect major participants, their correspondents, markets, and interdependent networks.

Operational risks should be controlled by the banks through a sound system of internal controls including physical security, data security, systems testing, segregation of duties, backup systems, and contingency planning. In addition, a comprehensive audit program to assess risks, adequacy of controls, and compliance with bank policies is essential.

Since most banks are third party participants in international networks, their ability to influence controls is limited. Nevertheless, they must recognize risks to their own business operations and compensate through their own internal controls. In addition, banks should exercise their influence over third party systems to the extent possible to insist upon sound operations for system continuity and integrity.

Comptroller of the Currency Administrator of National Banks

Banking Circular 260
Date: July 14, 1992

Subject: EDP Service Contracts

To: Chief Executive Officers of All National Banks, Deputy Comptrollers, District Administrators, Department and Division Heads, and all Examining Personnel

BACKGROUND

This issuance replaces BB 90-4 dated February 16, 1990. The FFIEC statement is unchanged.

SUMMARY

Attached is an "Interagency Statement on EDP Service Contracts" issued by the Federal Financial Institutions Examinations Council (FFIEC). This statement alerts financial institutions to potential risks in contracting for EDP services and failing to properly account for certain contract provisions.

Management of national banks is cautioned against contracting for services that include excessive fees or "inducement" provisions similar to those described in this statement. Furthermore, accounting for transactions under the contracts must conform to generally accepted accounting principles and call report instructions. This office considers contracting for excessive servicing fees, or failing to properly account for such transactions, an unsafe and unsound banking practice.

ORIGINATING OFFICE

Office of the Chief National Bank Examiner (202) 874-5170

/s/ Donald G. Coonley
Chief National Bank Examiner

See FFIEC Policies SP-6 for details.

Comptroller of the Currency Administrator of National Banks

Banking Circular 271
Date: May 25, 1993

Subject: EFT Switches and Network Services

To: Chief Executive Officers of All National Banks, Deputy Comptrollers, District Administrators, Department and Division Heads, and all Examining Personnel

PURPOSE

Attached is a joint statement by the Federal Financial Institutions Examination Council on risks associated with retail electronic funds transfer (EFT) switches and associated network services. EFT switches allow customer-initiated transactions to accounts through another institution's terminals, such as ATM or point-of-sale devices. The statement does not address wholesale or large dollar transfer systems.

The statement discusses some potential risks of such activities and possible ways to control them, both in the users' and the providers' operations. Each national bank EFT switch user and its processor are expected to maintain supervision and controls consistent with the guidelines in the statement.

POLICY

Examiners will schedule examinations of EFT switch and network service providers the same as for any other provider of data processing services to national banks. They will rely on applicable portions of the FFIEC EDP examination work program and the attached statement for procedures.

ORIGINATING OFFICE

Office of the Chief National Bank Examiner, (202) 874-5170

/s/Donald G. Coonley
Chief National Bank Examiner

See FFIEC Policies SP-9 for details.

Comptroller of the Currency Administrator of National Banks

**Examining Circular 238
Supplement 1
Date: August 2, 1989**

Subject: Specialty Rating Disclosure

**To: Deputy Comptrollers, District Administrators, Department and Division Heads
and All Examining Personnel**

PURPOSE

This supplement informs all examining personnel of a change in OCC policy regarding disclosure of trust, EDP, consumer compliance and Community Reinvestment Act (CRA) ratings to banks.

BACKGROUND

The OCC assigns ratings under uniform interagency rating systems for trust, data processing operations, consumer compliance and the Community Reinvestment Act. The trust, consumer compliance, and CRA ratings have not previously been disclosed to individual national banks. The EDP rating currently is not being disclosed to data centers.

POLICY

Effective immediately, the composite trust, consumer compliance and CRA ratings will be disclosed, in writing, to national banks (e.g., in the supervisory letter). The ratings will be assigned by the office that supervises the bank. Examiners should not disclose the ratings to the bank because recommended ratings are not final until approved by the supervisory office. Further, the examiner should not discuss the ratings with the bank; the ratings are not subject to negotiation. Individual component ratings should not be disclosed.

Composite ratings for data processing operations will be disclosed in writing to the bank or center examined. EDP ratings should not be disclosed to customers of the vendor. The ratings will be assigned by the office that supervises the data center. The examiner should not discuss the ratings with the data center. Individual component ratings should not be disclosed. This issuance does not change the report and distribution procedures established by Banking Circular 109 and Supplement 1 to that circular, which remain in effect.

The written communication should refer to the ratings definitions. The definitions may be included in the appendix to the ROSA or on a supplemental paper. Alternatively, the communication may refer to an external source (e.g., "see the FFIEC's EDP Examination Handbook, Section 14.3 for further information," or "see the Comptroller's Handbook for Consumer Examinations, Section 504.500 and 504.500 for further information").

Composite ratings assigned before the effective date of this supplement should not be disclosed. Ratings should be disclosed only going forward, as they are assigned, confirmed or changed. The supervisory office will decide when and how to inform the bank or data center of its ratings. Written communication should be made within a reasonable period after the rating is assigned.

The bank or data center should be cautioned that it may not disclose the ratings. Disclosure of the trust, EDP, consumer compliance, or CRA ratings by the bank's director, officers, etc., will be considered a violation of 12 C.F.R. 4.18 (c) and subject to penalties in 18 U.S.C. 641, as is disclosure of the contents of the Report of Supervisory Activity.

ORIGINATING OFFICE

Consumer Activities Division (202) 874 - 5190

/s/ Robert J. Herrmann
Senior Deputy Comptroller for Bank Supervision Policy

Comptroller of the Currency Administrator of National Banks

Examining Circular 261
Date: January 24, 1992

Subject: Interagency EDP Examination, Scheduling, and Report Distribution Policy

**To: Deputy Comptrollers, District Administrators, Department and Division Heads,
and all Examining Personnel**

PURPOSE:

Attached is a joint policy statement by the Federal Financial Institutions Examination Council (FFIEC). This policy updates procedures for joint or rotated examinations of data centers providing services to insured financial institutions supervised by more than one federal regulatory agency. It also provides policy for the administration of the Multiregional Data Processing Servicer (MDPS) program.

The attached policy statement replaces BC-109, dated May 31, 1978, and its supplement. It reflects only minor changes, except those concerning distribution of reports and, for MDPS, examination scheduling.

ORIGINATING OFFICE:

Office of the Chief National Bank Examiner, (202) 874-5170.

/s/Donald G. Coonley
Chief National Bank Examiner

See FFIEC Policies SP-1 for details.

Comptroller of the Currency Administrator of National Banks

Advisory Letter 88-7
Date: November 21, 1988

Subject: Large-Scale Integrated Financial Software Systems

To: Chief Executive Officers of All National Banks, Deputy Comptrollers, District Administrators and All Examining Personnel

PURPOSE

Attached is a joint issuance by the Federal Financial Institutions Examination Council. The paper discusses advantages and disadvantages associated with large-scale integrated financial software systems (LSIS). It alerts financial institutions to the potential risks and controls appropriate for the development, implementation and use of these systems.

LSIS systems are software products which combine several banking applications in one package. They are becoming more common, particularly among larger banks, as a means of improving the institution's competitive position and information systems. Bank executives and directors should be aware of and concerned about the potential problems with these systems. Banks using or considering LSIS should implement applicable supervision and controls, consistent with guidelines in this paper.

ORIGINATING OFFICE

EDP Activities Division

/s/Robert J. Herrmann
Senior Deputy Comptroller for Bank Supervision Policy

See FFIEC Policies SP-4 for details.

Comptroller of the Currency Administrator of National Banks

**Advisory Letter: 91-4
Date: July 24, 1991**

Subject: Social Security Numbers As Personal Identification Numbers

**To: The Chief Executive Officer and the Compliance Officer of Each National Bank
and all Examining Personnel.**

The purpose of this advisory is to alert you to the potential for security breaches or fraud through unauthorized access to customer accounts.

We are aware that some banks are allowing their customers to use the telephone to access account information and transfer funds between accounts. In many cases the customer only has to key in the account number and the last four digits of his or her social security number, which serves as the personal identification number (PIN). The use of the customer's social security number, or any other commonly used number, as the PIN, could make unauthorized access to customer accounts or frauds easier.

Social security numbers are now used in many states for driver license numbers or are required on the license. Many merchants who cash personal checks or accept payment by check require the customer's driver license number for identification purposes. As a result, anyone in possession of this information could access a customer's account.

We recommend that banks that offer telephone access to customer accounts devise PIN numbers that ensure adequate security for customer accounts. The use of social security numbers for PIN numbers may not safeguard account security for bank customers and could subject the bank to civil liability. In addition, national bank examiners may cite this practice as an internal control exception.

If you have any questions about this advisory please contact your supervisory office or the Compliance Management Department at (202) 874-4810.

/s/Phillip R. Freer, Jr.
Acting Deputy Comptroller for Compliance Management