

RESCINDED BC - 235

As of 10/1/2014, this guidance applies to federal savings associations in addition to national banks.

BANKING ISSUANCE

Comptroller of the Currency
Administrator of National Banks

Type: Banking Circular

Subject: International Payments Systems Risks

Replaced - See OCC 2021-49

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 banks 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.



BANKING ISSUANCE

Comptroller of the Currency
Administrator of National Banks

Type: Banking Circular

Subject: International Payments Systems Risks

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 systems;
- Ⓔ Establish a process to monitor on-going payments systems risks;
- Ⓕ 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

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

Attachment

INTERNATIONAL PAYMENT SYSTEMS RISK

APPENDIX

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

- ① credit (or counterparty) risks,
- ② sovereign risks, and
- ③ operational risks.

The control process 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 payments system. However, the success or failure of one system may affect others in the 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 in:

- ① Understanding the risks posed by participation in payment systems;
- ② Identifying bank policies designed to manage these risks; and
- ③ 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

CONTROL ISSUES

Management needs 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:

- ④ 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.
- ④ Controls to limit the overall exposure of the system, including debit cap limits.
- ④ 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.
- ④ Legal issues governing the system operation, including local laws, business practices, and government regulation.
- ④ 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.
- ④ Responsibility for reviewing the bank's participation in payment systems.

SETTLEMENT SYSTEMS

NET SETTLEMENT SYSTEMS

Net settlement systems 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 counterparties 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.

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.

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 member 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 on 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 outstanding 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 counterparties located in nations where this type of action is considered possible.

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 transactions. 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.