

PD-ABP-315  
94504

**Work Plan for Continued Assistance  
to National Securities Depository Limited**

**Financial Institutions Reform and  
Expansion (FIRE) Project**

**April 1997**

**Financial Institutions Reform and Expansion (FIRE) Project  
US Agency for International Development (USAID/India)  
Contract #386-0531-C-00-5010-00  
Project #386-0531-3-30069**

**Price Waterhouse LLP  
1616 North Fort Myer Drive  
Arlington, VA 22209  
Tel. (703) 741-1000  
Fax (703) 741-1616**

## *Price Waterhouse LLP*



April 15, 1997

Mr. C. B. Bhave  
Managing Director,  
National Securities Depository Limited  
Trade Towers, 4th floor  
Kamla Mills Compound  
Senapati Bapat Marg  
Mumbai 400 025.

Dear Mr. Bhave,

**Re: Work Plan for continued assistance to the National Securities  
Depository Limited (NSDL)**

At your request and as a part of our contract with the USAID, Ms. Susan Hertel, Former Vice President with the Midwest Clearing Corporation/ Midwest Securities Trust Company of the US and a consultant to Price Waterhouse Capital Markets, has completed the next part of our activity towards assisting the NSDL organizational setup.

### **Purpose of Activity**

The purpose of this activity was to develop a work plan addressing the organizational requirements and specifically the various training needs of NSDL. This was to be based on the current status of the development of the depository organization and as recommended by Price Waterhouse in the past to NSDL.

### **Approach to Work**

#### *a. Background*

Based on the Organizational Structure Plan (*the Plan*) submitted by Price Waterhouse to NSDL in July, 1996, NSDL has been establishing and staffing various departments within the depository.

The NSDL senior management has previously expressed an interest in receiving assistance from Price Waterhouse in training their management team and staff in various aspects of the securities depository environment.

Mr. C. B. Bhawe  
April 15, 1997

Page 2



NSDL senior management had agreed in November, 1996 that the training needs of the new organization should be addressed by Price Waterhouse. To provide a foundation for such training, in January, 1997, Price Waterhouse performed a review of the development of each department to date. The recommendations made on the basis of this review were published by Price Waterhouse under the title of Review of Organizational Development for the National Securities Depository Limited, March 1997.

During this visit Ms. Hertel continued to follow-up with NSDL on their progress, and met with senior NSDL management, to obtain a current status of the overall development of the organization.

*b. Review of organizational development*

Based on her review in her previous visit, a list of recommendations for support by Price Waterhouse was submitted to the NSDL senior management in March 1997.

These recommendations included the following:

- ▶ Assisting NSDL in meetings with issuers and R&T agents;
- ▶ Assisting NSDL in identifying areas of compliance, surveillance, and risk management to be addressed by the respective departments;
- ▶ Assisting NSDL in developing ongoing management reports to monitor growth and activity in the depository;
- ▶ Assisting in documenting formal procedures for each department;
- ▶ Assisting with various training issues, including: general management training in depository concepts in other countries, development of an overall orientation program to be administered by NSDL's Human Resources Department and obtaining technical training for systems staff;
- ▶ Assisting NSDL in fine-tuning the structure of each department; and
- ▶ Assisting with business continuity planning for business areas.

A further review of the organizational development of NSDL was conducted on the basis of discussions with the NSDL Management team. During the review, specific

Mr. C. B. Bhave  
April 15, 1997

Page 3



training needs and desires of the management and staff were identified. Areas of concern and difficulties being experienced by the staff in performing the operational procedures were also discussed with NSDL management.

Ms. Hertel obtained a consensus from NSDL management on the appropriateness of recommendations made in the plan.

### **Findings and Recommendations**

#### *a. Adjustments to the March recommendations*

The recommendations made in March 1997 were discussed with NSDL's Managing Director and Executive Director. (Individuals with whom these discussions took place may be found in Appendix A.) It was agreed that Price Waterhouse should proceed with the various areas of support.

Input was also received from the Executive Directors on any adjustments that should be made to the narrative included with the March recommendations. While most adjustments were based on changes at the depository since the previous review, Price Waterhouse was also advised that the Internal Audit function is being outsourced. During discussion on this practice, it was also determined that a business operations audit has not yet been performed at NSDL. Such an audit performed on an ongoing basis would strengthen the overall business operations of the depository. Tasks under the overall work plan will support this process.

#### *b. Next steps in organizational development - The Work Plan*

Based on these discussions, a work plan has been developed to systematically address each task over the next several months. (The actual work plan may be found in Appendix B). The status of the work plan will be updated and distributed to NSDL's senior management on a regular basis. Tasks and target/completion dates will be adjusted as needed. Additional or future areas of support may also be identified through this process.

### **Training Session on Compliance, Surveillance and Risk Management**

The first task of the work plan was performed in March, 1997. A training session was held on concepts of and approaches to work in the areas of compliance, surveillance, and risk management. (Attendees at this training session may be found in Appendix A.) Copies of publications were provided to the respective

Mr. C. B. Bhavé  
April 15, 1997

Page 4



department heads at NSDL. (Materials distributed may be found in Appendix C.) How certain techniques could be applied to the NSDL environment were discussed. The managers were left with an exercise to identify functions, responsibilities, and areas of exposure for each of their departments. This information will be used as a basis for additional work under the work plan.

Work on the remaining tasks under the work plan will begin in May, 1997.

### Next Steps

The work plan is designed around the currently identified training needs of NSDL. The plan includes target and completion dates for various activities to be performed.

Ms. Susan Hertel shall return to India in May, 1997. At that time, any additional concerns and ideas will be incorporated into the recommendations. Priorities and a schedule will be fine tuned at that time for the continued work.

Among other things during her next visit, Ms. Hertel will assist NSDL in creating a training package on the development of internal operating procedures and a training package on depository services provided in the United States.

These packages will be used for training sessions to be held on Ms. Hertel's next visit to India.

Besides the identified training sessions, She shall also assist NSDL in developing departmental operating procedures manuals. Depending on availability of NSDL management, this process will begin with 1 or 2 departments.

Both the training and the creation of the initial departmental procedure manuals will also give the depository management the tools to continue to document and maintain operational procedures under the evolution of the depository. Such procedures are extremely important for future training of staff, as a reference for day-to-day operations, and to support industry regulatory requirements.

For the success of this project the participation and cooperation of your management and staff is essential. We would like to thank you and your colleagues at NSDL and NSE for the time, courtesy and cooperation extended to us during the course of this project.

*Mr. C. B. Bhawe*  
*April 15, 1997*

*Page 5*



Please get in touch with us at the FIRE project for any clarifications you may require.

Thanking you,

Yours sincerely,

**W. Dennis Grubb**  
**Principal Consultant**

*Work Plan  
for Continued Assistance to  
National Securities Depository Limited*

*Price Waterhouse LLP  
Mumbai  
April 1997*

TABLE OF CONTENTS

**I. Executive Summary ..... 1**

**II. Background ..... 3**

**III. Work Plan ..... 5**

**IV. Training Session on Compliance, Surveillance, and  
Risk Management Issues ..... 6**

**V. Adjustments to the Report on Organizational Development  
based on Review of Recommendations with NSDL ..... 7**

**A. Systems ..... 7**

**B. Business Operations ..... 8**

**VI. Conclusion ..... 10**

**Appendices**

- A. Meetings Conducted and List of Attendees**
- B. Work Plan for NSDL**
- C. Training Materials on Compliance, Surveillance, and Risk  
Management**

## **I. EXECUTIVE SUMMARY**

The NSDL senior management has previously expressed an interest in receiving assistance from Price Waterhouse in training their management team and staff in various aspects of the securities depository environment. To provide a foundation for such training, in January, 1997, Price Waterhouse performed a review of the development of each department to date.

During the review, specific training needs and desires of the management and staff were identified. Areas of concern and difficulties being experienced by the staff in performing the operational procedures were also discussed with NSDL.

Based on this review, a list of recommendations for support by Price Waterhouse was submitted to the NSDL senior management (published by Price Waterhouse under the title of Review of Organizational Development for the National Securities Depository Limited, March 1997). These recommendations included:

- Assist NSDL in meetings with issuers and R&T agents.
- Assist in identifying areas of compliance, surveillance, and risk management to be addressed by the respective departments.
- Assist in developing ongoing management reports to monitor growth and activity in the depository.
- Document formal procedures for each department.
- Assist with various training issues, including
  - ▶ General management training in depository concepts in other countries.
  - ▶ Development of an overall orientation program to be administered by NSDL's Human Resources Department. This would include training for junior staff about depository concepts.
  - ▶ Obtaining technical training for systems staff. Specifically, this training would be on EDP audit and system security as training on these topics is limited in India.
  - ▶ Assistance is in fine-tuning the structure of each department.

- Assist with business continuity planning for business areas.

The recommendations were then discussed with NSDL's Managing Director and Executive Director. (Individuals with whom these discussions took place may be found in Appendix A.) It was agreed that Price Waterhouse should proceed with the various areas of support.

Based on these discussions, a work plan has been developed to systematically address each task over the next several months. (The actual work plan may be found in Appendix B). The status of the work plan will be updated and distributed to NSDL's senior management on a regular basis. Tasks and target/completion dates will be adjusted as needed. Additional or future areas of support may also be identified through this process.

The first task of the work plan was performed in March, 1997. A training session was held on concepts of and approaches to work in the areas of compliance, surveillance, and risk management. (Attendees at this training session may be found in Appendix A.) Copies of publications were provided to the respective department heads at NSDL. (Materials distributed may be found in Appendix C.) How certain techniques could be applied to the NSDL environment were discussed. The managers were left with an exercise to identify functions, responsibilities, and areas of exposure for each of their departments. This information will be used as a basis for additional work under the work plan.

Input was also received from the Executive Directors on any adjustments that should be made to the narrative included with the March recommendations. While most adjustments were based on changes at the depository since the review, Price Waterhouse was also advised that the Internal Audit function is being outsourced. During discussion on this practice, it was also determined that a business operations audit has not yet been performed at NSDL. Such an audit performed on an ongoing basis would strengthen the overall business operations of the depository. Tasks under the overall work plan will support this process.

Work on the remaining tasks under the work plan will begin in May, 1997.

70

## **II. BACKGROUND**

In January, 1997, an organizational review was performed by Price Waterhouse to determine the development status of each department and their current training needs. Recommendations were then made to the NSDL senior management team on training and other support could be provided by Price Waterhouse. These recommendations, published by Price Waterhouse under the title of Review of Organizational Development for the National Securities Depository Limited, March 1997, included:

- Security eligibility - Assist NSDL in soliciting issuers and R&T agents.
- Surveillance - Assist in identifying areas of surveillance to be addressed by this group.
- Risk Management - Assist in identifying areas to monitor.
- General management reports - Assist in developing ongoing management reports to monitor growth and activity in the depository. Such tools are critical to insuring the effectiveness of depository operations.
- Develop formal procedures - Assist in identifying tasks to document, train staff on how to write procedures, and possibly help with technical writing.
- Training Issues - Various levels of training are needed by NSDL. Examples are:
  - ▶ General management training in depository concepts. Comparison to what services are provided by other depositories is also desired.
  - ▶ Development of a training program for junior staff about depository concepts. This should be incorporated into an ongoing comprehensive orientation program. NSDL's HR department could then periodically give sessions for groups of new hires.
  - ▶ Obtaining technical training for systems staff - Systems management expressed a major concern about the lack of experience among their staff. More technical training is needed in the type of mainframe system being used by NSDL and how other large financial organizations use such systems, EDP audit process and system security. (This would be outside of support being given by NSDL's technical consultant.)

- ▶ Training by department - Assistance is needed by each department management in fine-tuning the structure of their department.
- Business continuity planning for business areas - Assist in setting up a BCP for business operations department. While NSDL is beginning to think about a BCP for the systems area, there still needs to be work done for the business operations.
- Compliance - Assist in developing areas for review/monitoring in depository operations to insure compliance with SEBI regulations.

In March, 1997, individual meetings were held with the members of the senior management team to review these recommendations as published and obtain agreement from NSDL management on the follow-up work to be done by Price Waterhouse. (Persons met with may be found in Appendix A.) The resulting primary deliverable is a work plan to address all of the areas.

A secondary deliverable in the form of a training session on compliance, surveillance and risk management issues. (Those who attended this session are listed in Appendix A.)

12

### **III. WORK PLAN**

Based on the agreement by NSDL to the Price Waterhouse recommendations, a work plan has been developed by Price Waterhouse to address the various training needs at NSDL. Other support to NSDL is also included in the work plan and will be provided on an ongoing basis as desired by NSDL.

The work plan includes target beginning and completion dates. Over the following several months, the work plan will be updated with the actual completion dates and distributed to the NSDL management team to keep them aware of the progress in meeting the various objectives. Adjustments to the work plan will also be made as necessary where priorities change and/or new areas of support are identified. The actual work plan may be found in Appendix B. Necessary meetings and training sessions will be schedule prior to the target month.

It is recognized that some of the tasks being completed under this work plan may appear to be a duplication of efforts in work being performed by another Price Waterhouse team in the area of EDP audit and controls. While some of the resources may be the same, the end products will be different. Price Waterhouse will strive to minimize the duplication of interviews of employees and insure that all overlapping work is coordinated so that the end results compliment each other.

#### **IV. TRAINING SESSION ON COMPLIANCE, SURVEILLANCE, AND RISK MANAGEMENT ISSUES**

During the last review and discussions, NSDL management in charge of Compliance, Surveillance, and Risk Management requested assistance in developing the responsibilities for their respective areas. The review found that little had been done to establish functions in these departments. This lack of definition of duties is normal under the early stages of the depository, but needs to be addressed soon by the depository.

A training session was held with the appropriate department heads at NSDL. The information provided was based on the consultant's experience in managing related areas within a U.S. depository. This was supplemented with various publications on these three topics. Discussion centered around how the ideas and approaches to risk and surveillance as presented in the publications might be applied to NSDL.

An exercise was left with the NSDL management team to be worked on over the next month. The attendees were provided with a sample chart used in the U.S. to identify areas to be addressed by the Risk Management area. Similar charts can be produced for Compliance and Surveillance. The ideas developed by the NSDL management team through this exercise will provide a basis for defining these three departments and documenting functional procedures under the proposed work plan.

Attendees at this training session may be found in Appendix A. Copies of the materials distributed at the session are located Appendix C.

**V. ADJUSTMENTS TO THE REPORT ON ORGANIZATIONAL DEVELOPMENT  
BASED ON REVIEW OF RECOMMENDATIONS WITH NSDL**

Individual meetings were held with the Managing Director and Executive Directors of both the Systems and Business Operations areas. (Meeting attendees can be found in Appendix A.) The recommendations specific to each area were discussed, and, in general, accepted. Training priorities were also established.

During these meetings, the following information was provided by NSDL to supplement the findings in the March report.

**A. Systems**

- Functions performed by the Computer Networking area in addition to those listed in the report include:
  - ▶ Maintenance of system security devices (encryption, message authentication, etc.)
  - ▶ DOT interface
  - ▶ Facilities system support to the depository in general
- Developing system efficiencies as noted in the report should be interpreted as monitoring the system resources.
- Functions under the Computer Systems area should be corrected as follows:
  - ▶ Installing hardware should be installing software
  - ▶ Integration testing should be interpreted as acceptance testing of new releases
  - ▶ Training of new users should be added to the list of responsibilities
- The Help Desk now interacts with 33 business partners (up from 16 at the time of the March report)
- In response to the system difficulties mentioned in the report, the following actions are being taken:
  - ▶

15

- ▶ Automation of software changes so that all changes are done for all users at one time.
- ▶ More organized releases of software changes through a quarterly schedule starting in June, 1997.
- ▶ Formalizing/expanding the Help Desk to take a proactive approach to advising all users of known software bugs and what work arounds should be used until programs are corrected.

Some software bugs are not reproducible so that they cannot be corrected immediately. They will continue to exist until the problem can be identified and reproduced. Therefore, NSDL has developed the above approach to assist users.

*Note: It was also noted by NSDL that all software problems are not related to the TCS applications. Some problems occur with the Microsoft software. The current feeling is that TCS is satisfactorily correcting all problems where the cause(s) can be identified.*

- ▶ Distribution of bulletins to users on known software bugs. Again, this takes a proactive approach the support of system users by the NSDL Systems area.
- NSDL advised that TCS is now providing documentation for certain pieces of the system. It is expected that this will continue satisfactorily until all needed documentation is received.
- The specific training needs for the Information Systems area were discussed further. It was agreed that FIRE would focus on identifying training resources for those topics that are generally not available in India. The subject matter should include data housing, data security, and EDP audit procedures. NSDL is especially interested in what software is used by other companies and how the selection process for specific software was conducted.

#### **B. Business Operations**

- The concept of an Internal Audit department was discussed. NSDL is currently outsourcing this function. The external auditor reviews certain areas of the depository on a monthly basis. The review is strictly on the financial aspects of the depository.

Usually, an Internal Audit department is part of the organizational structure of the depository, reporting to the Managing Director and, at times, the Board of Directors

16

directly. Having this auditing staff on site facilitates immediate needs to address real or perceived problems in addition to scheduled audits.

NSDL has elected to outsource this function to insure the integrity of the monthly reviews. There is a concern that an internal auditing staff may be biased in their opinions, favoring the operating departments. This is avoided by other organizations by having the work of the in-house Internal Audit department reviewed by external auditors as part of their periodic review.

Outsourcing the Internal Audit function may be workable

- ▶ if the availability of the auditor is flexible enough to meet emergency situations,
- ▶ if a second separate auditor is used for the external audit process, and
- ▶ if the outside Internal Auditor reports to the Board of Directors.

NSDL may find in the future that establishing this function in-house would be more cost-effective and convenient.

- Auditing concepts were further discussed as they pertain to the business operations of the depository. To date, audits have only reviewed the financial aspects of the business. Both internal and external auditors should also review the operational procedures and actual functions of the various operating departments within NSDL.

## **VI. CONCLUSION**

Price Waterhouse reviewed NSDL's departmental development and published recommendations in March, 1997. These recommendations were primarily based on current training needs of the depository, but other areas of potential support from Price Waterhouse were also included.

These recommendations were subsequently discussed with the senior management of NSDL. It was generally agreed that the recommendations were accepted and Price Waterhouse should proceed with the desired support to NSDL. Based on these discussions and agreements, a work plan has been developed to systematically address each training and other area over the next several months.

The work plan was actually begun in March, with a training session on compliance, surveillance, and risk management issues. During the departmental review, the department heads responsible for these areas requested ideas on functional responsibilities. (The respective departments are still in the development process as would be expected at this stage of the depository implementation.) Various publications on these topics were provided to the managers during this training session. Application of the approaches documented to the NSDL environment were discussed. The managers were left with an exercise to chart potential areas to be addressed by each department. The resulting documents will be used in identifying tasks on which to write procedures as called for under the work plan.

During the review of the recommendations with NSDL's senior management, input was received on adjustments that should be made to the March, 1997 report by Price Waterhouse. It was discovered during these discussions that NSDL continues to outsource the Internal Audit function and that a business operational audit has not yet been performed. While certain conditions may allow the outsourcing, Price Waterhouse strongly urges NSDL to have the business operations audited. The procedures and other tasks under the work plan will facilitate this process.

Additional tasks under the work plan will commence in May, 1997.

**APPENDICES**

**List of Appendices**

- A. Meetings Conducted and List of Attendees**
- B. Work Plan for NSDL**
- C. Training Materials on Compliance, Surveillance, and Risk Management**

**APPENDIX A**

**MEETINGS CONDUCTED AND THE LIST OF ATTENDEES**

## **APPENDIX A**

### **MEETINGS CONDUCTED AND LIST OF ATTENDEES**

#### **National Securities Depository Limited - Review of Recommendations**

C. B. Bhave, Managing Director  
Gagan Rai, Executive Director, Business Operations  
Rajesh Doshi, Executive Director, Systems

#### **Training Session for NSDL on Compliance, Surveillance, and Risk Management**

Rajesh Doshi, Executive Director, Systems  
Shashikant Shirhati, Vice President, Systems  
Mukesh Mistry, Vice President, Systems  
T. Koshy, Vice President, Marketing and Risk Management  
Jayesh Sule, Assistant Vice President, Personnel and Participant Interface  
S. Gopalan, Assistant Vice President, Issuer Interface and Compliance

**APPENDIX B**

**WORK PLAN FOR NSDL**

**APPENDIX B**

**WORK PLAN FOR NSDL**

<b>TASK</b>	<b>TARGET START DATE</b>	<b>TARGET COMPLETE DATE</b>	<b>ACTUAL COMPLETE DATE</b>
Training session on Compliance, Surveillance, and Risk Management	March, 1997	March, 1997	March, 1997
Training session on securities depository services in the U.S.	May, 1997	July, 1997	
Training session on procedure documentation	May, 1997	May, 1997	
Identify training resources within/outside India for specific topics as needed by NSDL	May, 1997	Ongoing	Ongoing
Documentation of departmental procedures			
Issuer Interface	May, 1997	July, 1997	
Participant Interface	May, 1997	July, 1997	
Clearing Corporation Interface	July, 1997	September, 1997	
Corporate Communications	July, 1997	September, 1997	
Compliance	July, 1997	September, 1997	
Finance	July, 1997	September, 1997	

Surveillance	September, 1997	November, 1997	
Risk Management	September, 1997	November, 1997	
Establish Human Resources orientation program	July, 1997	September, 1997	
Review/create management reports	November, 1997	January, 1998	
Assist in meetings with issuers and R&T agents to solicit participation in the depository	Ongoing as needed by NSDL	Ongoing	Ongoing
Assist in development of Business Continuity Plan for business operations	November, 1997	January, 1998	
Computer Networking	As needed to support out-sourced technical work	As needed to support out-sourced technical work	
Computer Systems	As needed to support out-sourced technical work	As needed to support out-sourced technical work	

25



# Financial Integrity Recommendations

For Futures and Options Markets and Market Participants



**Futures Industry Association  
Global Task Force  
on Financial Integrity**



**FIA TASK FORCE  
RECOMMENDATIONS**

June 1995

On behalf of the Futures Industry Association Global Task Force on Financial Integrity, I am pleased to present the recommendations for futures and options exchanges/clearinghouses, brokers/intermediaries and customers. These recommendations, which were developed through the efforts of more than 60 participants from 17 jurisdictions, represent an unprecedented international initiative for the financial services industry.

These 60 recommendations reflect the contributions of futures and options organizations in Australia, Belgium, Canada, France, Germany, Hong Kong, Italy, Japan, the Netherlands, New Zealand, Norway, Singapore, South Africa, Spain, Sweden, the United Kingdom and the United States.

I would like to thank the sponsors of the Task Force and recognize the efforts of the representatives from various exchanges/clearinghouses, brokerage firms and institutions that have participated in this process either by responding to questionnaires or attending the meetings in Washington, D.C. and London.

We are pleased with the response and are confident that these recommendations will help us improve the financial integrity of our industry for all participants.

Michael G. Philipp  
Chairman  
FIA Global Task Force  
on Financial Integrity

## FIA Global Task Force on Financial Integrity

### Chairman

**Michael G. Philipp**  
Former Managing  
Director  
Merrill Lynch Futures Inc.

### Members

**Amsterdam Futures**  
• M.P.A. De Vries  
**BELFOX**  
• W. Van Stappen  
**Board of Trade  
Clearing Corporation**  
• Dennis A. Dutterer  
• John C. Hiatt  
**Cargill Investor Services,  
Inc.**  
• Hal T. Hansen  
**Chase Manhattan  
Futures Corp.**  
• Janice C. Abrahamson  
**Chicago Board of Trade**  
• Carol A. Burke  
• Ralph I. Goldenberg  
• Kathryn M. Trkla  
**Chicago Mercantile  
Exchange**  
• Eileen T. Flaherty  
• Kathryn J. Meyer  
**Coffee, Sugar & Cocoa  
Exchange, Inc.**  
• Audrey Hirschfeld  
**Dean Witter Reynolds**  
• Laurence E. Mollner  
**Deutsche Borse AG**  
• Michael Hofmann  
• Anselm Jumpertz  
**FIMAT Futures USA**  
• Gary Alan DeWaal  
**FIA Board of Directors**  
• Robert E. Zellner  
**Futures Industry  
Association**  
• Mary Ann Burns  
• John M. Damgard  
• Barbara Wierzynski  
**Futures Industry  
Institute**  
• Paula A. Tosini  
**Futures and Options  
Association**  
• Anthony Belchambers

**General Motors  
Investment Management  
Corporation**  
• William P. Miller II  
**Harris Futures  
Corporation**  
• Jennifer S. Johnson  
**Harvard Management  
Company, Inc.**  
• Michael Pradko  
• Verne O. Sedlacek  
**Hong Kong Futures  
Exchange**  
• Ivers W. Riley  
**Italian Stock Exchange  
Council**  
• Luigi Ruggerone  
**John W. Henry  
& Co., Inc.**  
• Peter F. Karpen  
**Lehman Brothers Inc.**  
• Ronald H. Filler  
• Charles P. Nastro  
**London Clearing House**  
• David M. Hardy  
• Andrew Lamb  
**London Commodity  
Exchange**  
• Michael N. Jenkins  
**London International  
Financial Futures &  
Options Exchange**  
• Daniel Hodson  
• Nick Carew Hunt  
• Richard Pratt  
**London Metal Exchange**  
• Neil D. Banks  
**Managed Futures  
Association**  
• L. Carlton Anderson  
• Clyde F. Ensslin  
**MATIF**  
• Louis-Armand de Rouge  
• Michel Favreau  
• Patrick Stephan

**Merrill Lynch  
Futures Inc.**  
• William T. Maitland  
**Merrill Lynch Japan Inc.**  
• David J. Semaya  
**Montreal Exchange**  
• John S. Ballard  
**Morgan Stanley & Co.**  
• John P. Davidson III  
**National Futures  
Association**  
• Daniel A. Driscoll  
**New York Mercantile  
Exchange**  
• Bernard J. Purta  
• Neal L. Wolkoff  
**Northern Futures  
Corporation**  
• David R. Ganis  
**OMLX, The London  
Securities and  
Derivatives Exchange**  
• Derek Oliver  
**OM Group**  
• Hans Berggren  
**Refco Commodities  
Services GMBH**  
• Elizabeth Ocker  
**Refco Overseas Ltd.**  
• Richard A. Reinert  
**Sakura Dellsler, Inc.**  
• Karen M. Dorff  
• Leo Melamed  
**Salomon Brothers Inc**  
• Marcy Engel  
**Smith Barney Inc.**  
• Steven Keltz  
**Sydney Futures Exchange**  
• Terrence F. Martell

---

*Counsel to the Task Force:*  
**Sullivan & Cromwell**  
• Kenneth M. Raisler  
• David J. Gilberg  
• William Y. Chua



## Sponsors

- Chicago Board of Trade
- Chicago Mercantile Exchange
- Coffee, Sugar & Cocoa Exchange, Inc.
- Deutsche Borse AG
- ECOFEX
- Futures Industry Association
- Hong Kong Futures Exchange
- International Petroleum Exchange of London Ltd.
- Kansas City Board of Trade
- The London Clearing House
- London Commodity Exchange
- London International Financial Futures & Options Exchange
- London Metal Exchange
- MATIF
- Managed Futures Association
- Minneapolis Grain Exchange
- The Montreal Exchange
- National Futures Association
- New York Cotton Exchange
- New York Mercantile Exchange
- OMLX, The London Securities and Derivatives Exchange
- Singapore International Monetary Exchange Ltd.
- South African Futures Exchange
- Sydney Futures Exchange

## Exchange/Clearinghouse Respondents

- Amsterdam Futures
- BELFOX
- Chicago Board of Trade
- Chicago Mercantile Exchange
- Coffee, Sugar & Cocoa Exchange, Inc.
- Deutsche Borse AG
- The FUTOP Clearing Centre
- Hong Kong Futures Exchange
- International Petroleum Exchange of London Ltd.
- Italian Stock Exchange Council
- The London Clearing House
- London International Financial Futures & Options Exchange
- London Metal Exchange
- MATIF
- MEFF Renta Fija
- Minneapolis Grain Exchange
- Montreal Exchange
- New York Cotton Exchange
- New York Mercantile Exchange
- New Zealand Futures & Options Exchange Limited
- OM Group
- OMLX, The London Securities and Derivatives Exchange
- Oslo Exchange
- Osaka Securities Exchange
- Singapore International Monetary Exchange Ltd.
- South African Futures Exchange
- Sydney Futures Exchange
- Tokyo Commodity Exchange
- Tokyo Grain Exchange
- Tokyo International Financial Futures Exchange
- Tokyo Stock Exchange
- Vancouver Stock Exchange

## Acknowledgements

The Futures Industry Association is grateful for the support and volunteer hours devoted by the many exchange, clearinghouse, broker, intermediary and customer representatives to respond to the questionnaires, discuss the issues and reach a consensus on the recommendations. The FIA would like to acknowledge:

- The 41 global brokers/intermediaries and 28 end users from 8 jurisdictions that responded to questionnaires and participated in interviews on a confidential basis.
- The members of the FIA board of directors and in particular the efforts of FIA Chairman Peter F. Karpen, John W. Henry & Co., Inc.; the Financial Integrity Committee; public director Verne O. Sedlacek, Harvard Management Company, for chairing the customer response; and Hal T. Hansen, Cargill Investor Services, for chairing the broker/intermediary response.
- The Futures and Options Association, particularly Anthony Belchambers, for coordinating the U.K. exchange, brokerage and customer responses.
- The FIA Japan Chapter for translating the surveys and interviewing intermediaries and customers in Japan.
- The FIA Law & Compliance Division for their counsel.
- Gerald A. Tellefsen, Tellefsen Consulting Group, for organizational and conceptual assistance.

## Introduction

---

In February 1995 Barings PLC, an international financial institution with a 200-year history, collapsed as a result of substantial trading losses incurred by a Barings employee. These losses were caused in large part by a lack of adequate internal controls over the employee's proprietary trading activities, including those conducted in exchange-traded futures and options. The Barings failure did not result in losses to other market participants and, in many respects, the situation underscored the fundamental strength and soundness of the global futures and options regulatory, trading and clearing systems. Nevertheless, the events surrounding the Barings failure prompted market participants to consider certain national and cross-border issues related to the structure and operation of the international markets for exchange-traded and/or cleared futures and options. The most significant of these issues included the mechanisms that exist for the protection of participants' assets, the internal controls and risk management procedures employed by exchanges/clearinghouses, brokers/intermediaries and customers, and the communication of information regarding the activities of market participants by exchanges/clearinghouses and regulatory authorities.

The Futures Industry Association Global Task Force on Financial Integrity was organized in March 1995 to address these issues. The Task Force includes representatives of major international exchanges/clearinghouses, brokers/intermediaries (including futures commission merchants and other brokers), and customers from 17 jurisdictions.

### Task Force Objectives

The Task Force strongly believes that the global futures and options markets offer significant advantages and protections, such as transparency, liquidity and the elimination of direct credit exposure to trading counterparties, many of which are not present in other markets. These features, among others, promote confidence in the markets and provide an efficient environment in which to transact business. The primary goal of the Task Force is to enhance the protection of the assets of market participants and, as a means of achieving this objective, to:

- provide information and education about the global futures and options markets;
- provide market participants with a means of evaluating and comparing exchanges/clearinghouses and brokers/intermediaries;
- improve cross-border coordination and communication among exchanges/clearinghouses and regulators in the same and different jurisdictions, as well as the level of information available regarding the activities of market participants;

## Introduction

---

In February 1995 Barings PLC, an international financial institution with a 200-year history, collapsed as a result of substantial trading losses incurred by a Barings employee. These losses were caused in large part by a lack of adequate internal controls over the employee's proprietary trading activities, including those conducted in exchange-traded futures and options. The Barings failure did not result in losses to other market participants and, in many respects, the situation underscored the fundamental strength and soundness of the global futures and options regulatory, trading and clearing systems. Nevertheless, the events surrounding the Barings failure prompted market participants to consider certain national and cross-border issues related to the structure and operation of the international markets for exchange-traded and/or cleared futures and options. The most significant of these issues included the mechanisms that exist for the protection of participants' assets, the internal controls and risk management procedures employed by exchanges/clearinghouses, brokers/intermediaries and customers, and the communication of information regarding the activities of market participants by exchanges/clearinghouses and regulatory authorities.

The Futures Industry Association Global Task Force on Financial Integrity was organized in March 1995 to address these issues. The Task Force includes representatives of major international exchanges/clearinghouses, brokers/intermediaries (including futures commission merchants and other brokers), and customers from 17 jurisdictions.

### Task Force Objectives

The Task Force strongly believes that the global futures and options markets offer significant advantages and protections, such as transparency, liquidity and the elimination of direct credit exposure to trading counterparties, many of which are not present in other markets. These features, among others, promote confidence in the markets and provide an efficient environment in which to transact business. The primary goal of the Task Force is to enhance the protection of the assets of market participants and, as a means of achieving this objective, to:

- provide information and education about the global futures and options markets;
- provide market participants with a means of evaluating and comparing exchanges/clearinghouses and brokers/intermediaries;
- improve cross-border coordination and communication among exchanges/clearinghouses and regulators in the same and different jurisdictions, as well as the level of information available regarding the activities of market participants;

- promote, where necessary, changes in existing laws or regulations to facilitate the realization of the objectives;
- improve internal risk management by brokers/intermediaries of exposure to customer positions;
- improve internal risk management by brokers/intermediaries and customers of their own trading activities, including the activities of affiliates (proprietary trading); and
- enhance public confidence in the global exchange-traded futures and options markets.

The objectives of the Task Force are similar to those of the international regulatory authorities that issued the "Windsor Declaration" in May 1995.

### **Task Force Structure**

The Task Force has focused its examination on the global markets for futures and options executed on and/or cleared by organized exchanges/clearinghouses. The organization of the Task Force and its recommendations reflect the fundamental structure of the global futures and options markets. These markets are typically structured around a centralized exchange and/or clearinghouse, which is responsible for the clearance and settlement of such transactions and the financial obligations of the participants. On most markets, the exchange/clearinghouse maintains a direct legal relationship only with its members, not with the ultimate customers. The rules, oversight and market protection mechanisms of the exchange/clearinghouse generally extend only to its members, and any benefits or obligations regarding customers arise indirectly as a result of the relationships between the customers and their clearing members.

The Task Force is divided into three committees —exchanges/clearinghouses, brokers/intermediaries and customers. Each committee prepared a separate survey that was disseminated to a large number of market participants. These surveys generated responses from all sectors of the global futures and options industry and provided the Task Force with extensive information on the structure and operations of markets and their participants. The Task Force used the responses to develop its recommendations during a series of meetings, including sessions held in Washington, D.C. in May 1995 and in London in June 1995.



The recommendations are based on the principle that exchanges/clearing-houses, brokers/intermediaries and customers each have responsibilities with respect to their own activities and the operation of the system as a whole and that the markets function effectively only when market participants at all levels fulfill these responsibilities. For this reason, the three areas addressed below are interrelated and should be considered as a single integrated set of recommendations. The Task Force believes that the implementation of these recommendations will significantly advance the objectives of the Task Force.

### **Task Force Intent**

The Task Force recommendations are intended to provide general guidance to market participants regarding issues and principles which the Task Force believes should be taken into consideration by such participants in structuring their activities. The Task Force does not intend the recommendations to be construed as definitive requirements that must be met by regulatory systems, markets or market participants, or to identify deficiencies in any particular regulatory systems, markets or institutions. Each exchange, clearinghouse, broker/intermediary and customer must develop its own policies and procedures that are appropriate in the context of its particular laws, practices and circumstances.

The Task Force recognizes that no one approach can be appropriate for all markets or participants. In fact, some recommendations may be unnecessary or even inappropriate for brokers/intermediaries and customers whose activities in the futures and options markets are limited; market participants should evaluate the costs and benefits of these recommendations in light of their exposure to the markets relative to their overall businesses. The Task Force also recognizes that it may be appropriate for exchanges/clearinghouses, brokers/intermediaries or customers to rely, at least in part, on the strength of the regulatory and oversight system governing a market and the activities of market participants. In certain instances, the existence of such a regulatory and oversight system may address a number of the issues raised by the recommendations.

In addition, while there will continue to be important and fundamental differences among the laws and practices of various jurisdictions, the Task Force expects there to be improved coordination structured around the financial integrity objectives reflected in its recommendations. Further, where existing laws or regulations prevent or inhibit the implementation of appropriate recommendations, the Task Force urges legislators or regulators to change such laws or regulations.

The Task Force expects to issue a final report, which will contain further explanations and additional information compiled by the Task Force, in the next several months. At that time, the Task Force will determine whether any additional actions are appropriate.

# Recommendations For Regulators\*, Exchanges and Clearinghouses

## Financial Integrity Issues

### Member and Customer Protection

**1** Each exchange/clearinghouse and/or regulatory authority should have and maintain appropriate mechanisms designed to identify and protect clearing member and customer property in respect of instruments that are traded and/or cleared under the rules of the exchange/clearinghouse against dissipation as a result of the activities of brokers/intermediaries and their affiliates. Such mechanisms should enable the exchange/clearinghouse or regulatory authority to facilitate the transfer or close out of positions and the return of clearing member or customer property, or other appropriate actions, as promptly as feasible upon the cessation of business or insolvency of a clearing member or other broker/intermediary. Relevant mechanisms used by exchanges/clearinghouses might include trade registration requirements, recordkeeping requirements for carrying and/or clearing firms calling for the identification of customer positions and property, segregation of customer property, sufficient guarantees by credible sources, insurance of customer accounts or compensation funds. Regulatory authorities should facilitate the use of appropriate mechanisms by exchanges/clearinghouses:

**2** In the event of a default by a clearing member, the level of resources available to the exchange/clearinghouse should be sufficient to protect non-defaulting clearing members, and thereby their customers, against loss and to permit trading, settlement and clearing to continue without interruption. Such resources should be sufficient in light of market conditions and practices and should consist of liquid assets and/or committed lines of credit that are readily available for prompt application.

### Margin Requirements

**3** The primary purpose of an exchange/clearinghouse margin system should be the preservation and enhancement of the financial integrity of its marketplace. Margin requirements should be established through the use of risk-based systems that evaluate portfolios based on, among other criteria, pricing and volatility models. Such systems should provide the necessary flexibility to allow the exchange/clearinghouse to make prudential judgments regarding the appropriate level of margins for its market. The parameters of each pricing model should take into account, among other things, the timing of margin, settlement and other payment obligations in the relevant market. All open positions should be marked-to market no less than daily.

\* It should be noted that some recommendations made by the Task Force refer to regulators, exchanges and/or clearing houses collectively. A particular recommendation may deal with an exchange/clearing house in its capacity as such or in its capacity as a regulator. Further, in a number of jurisdictions, exchanges and/or clearing houses might be the primary market regulators in the absence of any governmental bodies with authority over the futures or options markets.

Each

exchange/clearinghouse  
and/or regulatory  
authority should  
maintain appropriate  
mechanisms designed  
to identify and protect  
customer funds.

Guarantee



4 Except where appropriate and legally permissible credit arrangements have previously been established, exchanges/clearinghouses or regulatory authorities should require that clearing members collect margin promptly from customers. In those instances in which margin is not collected within a reasonable period of time, exchanges/clearinghouses or regulatory authorities should require appropriate adjustments, which may include capital charges or additional collateral, to be made by such clearing members to reflect the potential exposure of such clearing members to their customers.

5 Payments obligated to be made to and from a clearinghouse should be irrevocable as of a time certain. Such payments should be made simultaneously or as close to simultaneously as is reasonably practicable in light of local market practices and needs.

**Dissemination of Information**

6 Each exchange/clearinghouse should make publicly available and periodically update information regarding its market protection mechanisms including:

- (a) the scope and operation of the market protection mechanisms;
- (b) the market participants covered by such mechanisms (including the applicability of such mechanisms to customers) and the extent to which such participants are covered; and
- (c) relevant bankruptcy law issues and treatment within its jurisdiction.

*Each exchange/clearinghouse should make publicly available information regarding its market protection mechanisms, a list of sources of financial support and financial information about the exchange/clearinghouse.*

7 Each exchange/clearinghouse should make publicly available and periodically update a list of the sources of financial support available to it as part of the applicable financial integrity system and the amount available from, and the liquidity of, each such source. The order in which such sources will be drawn upon, whether such sources must be repaid (and by whom) and any limits on the right to draw on such sources should be included in the information made available.

8 Each exchange/clearinghouse should make publicly available and periodically update financial information regarding the exchange/clearinghouse. The financial information should include reasonably sufficient information to permit market participants to evaluate the credit risk of the exchange/clearinghouse, to evaluate changes over time and to make appropriate comparisons among various exchanges/clearinghouses.

*9* X

**Transfers of Customer Positions and Property**

9 Each exchange/clearinghouse and/or regulatory authority should have in place rules and procedures to enable it to take appropriate actions to protect itself, its clearing members and thereby customer positions and property where a broker/intermediary is experiencing financial problems. Such actions might include effecting the transfer of positions and property from such broker/intermediary to a broker/intermediary in a stronger financial condition, or otherwise imposing additional financial or operational requirements and limitations on such broker/intermediary.

*10* X

10 In the event of a broker/intermediary's cessation of business or default, an exchange/clearinghouse and/or regulatory authority should have both the regulatory authority and the processing capability to require either the prompt transfer of customer positions and assets to another broker/intermediary or the close out of open positions. The manner in which such transfers or close outs are effected, including the pricing of such transfers or close outs, should be determined in accordance with a procedure that, to the fullest extent possible, has been established in advance and has been made known to market participants.

Each exchange/clearinghouse should have in place procedures and systems for the sharing of information regarding market participants and their trading activities

*11* X

**Exchange/Clearinghouse Risk Assessment; Reporting and Coordination**

**Information Sharing/Coordination**

11 Each exchange/clearinghouse should, subject to applicable law, have in place procedures and systems for the sharing of information regarding market participants and their trading activities, either directly or through the applicable regulatory authorities, with other exchanges/clearinghouses (including both futures and securities exchanges) and regulators, in the same and in other jurisdictions. Regulatory authorities should establish systems for the sharing of information with exchanges/clearinghouses and other regulatory authorities in the same and different jurisdictions regarding market participants and their trading activities. All information provided regarding market participants should be maintained in strictest confidence and on the condition that it not be used for commercial purposes.

*12* X

12 Regulatory authorities and/or legislators should effect any changes to existing laws and regulations that are necessary to permit exchanges/clearinghouses to share information with other exchanges/clearinghouses and/or other regulatory authorities for the purposes described herein.

13 If a market participant seeks to obtain financial, position, margin or other benefits from holding positions in similar instruments on more than one exchange, either for hedging or arbitrage purposes or for other reasons, each exchange/clearinghouse where beneficial treatment is sought should confirm the nature and existence of the market participant's positions in such instruments on other exchanges/clearinghouses. Such confirmation may, where appropriate, be based on information or documentation obtained directly from the market participant. In addition, however, the confirmation procedures used by the exchange/clearinghouse should include the ability, where necessary, to access information from the other exchange/clearinghouse on a confidential basis and on the condition that it not be used for commercial purposes. On the same terms, an exchange/clearinghouse also should confirm the nature and existence of over-the-counter or other instruments if they form the basis for beneficial treatment.

*to*

*Summary* X  
Each exchange/clearinghouse should be audited by an independent, external auditor on at least an annual basis.

14 Each exchange/clearinghouse and/or regulatory authority should develop and coordinate emergency action procedures to respond to crises in their markets or in other markets that may impact their markets. In developing these procedures, exchanges, clearinghouses and regulatory authorities should consider the use of mechanisms for the prompt transfer or close out of positions and the transfer of customer property. The operational aspects of these procedures should be tested on a regular basis.

**Audits/Reviews**

15 Each exchange/clearinghouse should be audited by an independent, external auditor on at least an annual basis. The relevant regulatory authorities should conduct routine reviews of the principal functions of exchanges and clearinghouses within their jurisdiction. Audits and reviews should include examinations of, among other matters, the risk management and market surveillance procedures, internal controls and financial condition of each exchange/clearinghouse.

*Summary* X  
*Periodic*  
*External*  
*Audits*  
*Required*

16 Each exchange/clearinghouse and/or regulatory authority, as appropriate, should conduct periodic audits of all clearing member firms. In addition, each exchange, clearinghouse and/or regulatory authority, as appropriate, should conduct periodic audits of any other entities within its jurisdiction that carry customer positions. Such audits should include, at a minimum, reviews of internal controls, risk management procedures and compliance with customer protection requirements.

*Summary* X

**Exchange/Clearinghouse Risk Assessment**

- Sum.*  
*Post*
- \* 17 Each exchange/clearinghouse should establish minimum financial requirements for member firms and should conduct at least daily reviews of such firms' positions at the exchange/clearinghouse in relation to their financial condition, amongst other criteria. In addition, each exchange/clearinghouse should establish other requirements and/or limitations, as appropriate, which may include position and concentration limits based on financial condition, to manage the risks of member firms' trading activities. Each exchange/clearinghouse should also have and enforce appropriate procedures to separate internal risk management personnel from personnel with marketing responsibilities. \* Regulatory authorities should recognize the benefits of risk-based financial requirements.

Regulatory  
authorities should have  
ready access, on a  
need to know basis,  
to the size and ultimate  
beneficial ownership of  
customer positions,  
including the positions  
of customers carried in  
or through omnibus  
accounts.

- ✕ 18 Regulatory authorities should have ready access, on a need to know basis, to the size and ultimate beneficial ownership of customer positions, including the positions of customers carried in or through omnibus accounts. In the event such information is not made available to an exchange/clearinghouse, it should be able to impose on the clearing member carrying the account either additional financial requirements and/or appropriate limitations on trading. Regulatory authorities and/or legislators should effect any necessary changes to existing laws or regulations to facilitate access by exchanges/clearinghouses to information on the size and ultimate beneficial ownership of customer positions. *Sum.*

- ✕ 19 In those markets where segregation is used as a customer protection mechanism, each exchange, clearinghouse and/or regulatory authority should preclude the commingling of segregated customer positions and proprietary positions of the broker/intermediary or its affiliates in omnibus accounts, by the carrying firm. Gross margining of positions held in omnibus accounts should be required at the level of the initial broker/intermediary carrying customer accounts and margin should not be permitted to be netted between segregated customer and proprietary omnibus accounts. In those markets where segregation is not applicable, other mechanisms to identify and protect customer funds and property, which may include the use of separate customer and proprietary accounts at depositories, should be used. *Sum.*

- 20 Each exchange/clearinghouse should establish and maintain standards of creditworthiness for eligible depository institutions holding clearing members' property on behalf of the clearinghouse.

## Legal/Regulatory Issues

### Bankruptcy Issues

- 21** The bankruptcy or other relevant laws of each jurisdiction should provide for (or at least not prevent) the prompt close out of positions and/or transfer of customer positions and property from a defaulted broker/intermediary to another broker/intermediary. Where necessary, exemptions from any automatic “stay” or similar provisions should be implemented in order to permit such transfers or close outs to be made.
- 22** The bankruptcy or other relevant laws of each jurisdiction should clearly specify the rights of customers and brokers/intermediaries upon the default of a clearinghouse, broker/intermediary or depository with respect to the customer and proprietary assets held by such clearinghouse, broker/intermediary or depository, including any priority rights granted to customers with respect to such assets.
- 23** Margin or settlement payments made to or from a broker/intermediary or exchange/clearinghouse should be protected from reversal in a bankruptcy proceeding.
- 24** Legislators and regulatory authorities should attempt to harmonize conflicting bankruptcy regimes in different jurisdictions in order to provide, to the maximum extent possible, for consistent treatment of customer positions and property upon the bankruptcy of a clearinghouse, a depository or a broker/intermediary. In addition, the bankruptcy or other relevant laws should ensure that brokers/intermediaries and clearinghouses are permitted to exercise rights of netting and set-off in the event of a default by a customer, broker/intermediary or clearinghouse.
- ### Coordination and Oversight by Regulatory Authorities
- 25** Regulatory authorities in different jurisdictions should, to the extent practicable, harmonize conflicting regulatory requirements with respect to market participants operating or trading in multiple jurisdictions. As part of this effort, regulatory authorities in each jurisdiction should clarify the scope of their authority with respect to domestic persons trading or engaging in other activities outside the jurisdiction and with respect to the trading or other activities of non-domestic persons within the jurisdiction.
- 26** Appropriate systems of regulatory oversight (which may include delegations of oversight responsibilities to exchanges, clearinghouses or other self-regulatory organizations) should be established and enforced in each jurisdiction. Such systems should include oversight and periodic reviews of the operations and activities of exchanges, clearinghouses, brokers/intermediaries and, where appropriate, other market participants.

---

*The bankruptcy or other relevant laws of each jurisdiction should provide for (or at least not prevent) the prompt close out of positions and/or transfer of customer positions and property from a defaulted broker/intermediary to another broker/intermediary.*



# Recommendations For Brokers and Intermediaries

## Risk Management: Exchanges/Clearinghouses, Clearing Brokers and Depositories

### Risk Assessment of Exchanges/Clearinghouses

**27** Brokers/intermediaries should consider information available about the risks of trading on a particular exchange/clearinghouse prior to executing trades on such market. Such risks should be monitored on an ongoing basis.

**28** Among the factors that might be appropriate to consider in determining whether to transact on a particular exchange/clearinghouse are the quality of the regulatory and oversight system of the exchange/clearinghouse; the applicable financial integrity system, relevant customer protection mechanisms (e.g., segregation requirements, account insurance, guarantees or compensation funds); the source and liquidity of relevant financial support; the margining and settlement system; the ability to transfer positions and property in the event of a default; the ability of the exchange/clearinghouse to impose capital requirements on its members, to require its members to increase their capital, or to assess its members; the description of the clearing members, and/or shareholders; and the regulatory and legal system including applicable bankruptcy laws in the relevant jurisdiction.

### **29** Risk Assessment of Clearing Brokers

Brokers/intermediaries should consider the financial condition, operational capacity and other material risks of the clearing brokers through which they execute and/or clear transactions on those markets where they do not clear directly (or through affiliates). The primary factors to consider in evaluating a clearing broker should include, among others, its credit standing, capital and financial condition, the exchanges/clearinghouses of which it is a member and the type of firm (for example, a bank, securities broker, insurance company or an affiliate thereof). Other factors that might also be considered include the clearing broker's management experience and capabilities, its margin policies and customer credit procedures, its operational capacity, risk management systems and disaster recovery procedures and whether or not it engages in proprietary trading. Based on the results of this consideration, brokers/intermediaries may consider implementing procedures, to be applied in appropriate instances, to protect against the risks of clearing through certain clearing brokers or categories of clearing brokers.

Brokers/intermediaries  
should consider  
information available  
about the risks of  
trading on a particular  
exchange/clearinghouse  
prior to executing  
trades on such market.



- 30 Those brokers/intermediaries with substantial exposure to clearing brokers as a result of the brokers/intermediaries' trading activities with such clearing brokers should establish and maintain back-up clearing relationships with other clearing brokers to be utilized in emergency situations. Such relationships should include completed contractual arrangements with such back-up clearing brokers and periodic testing of procedures for transfers of positions and property and continuation of trading.

**Risk Assessment of Depositories**

- \* 31 Brokers/intermediaries should consider and monitor on an ongoing basis the depositories utilized for custody of customer property. Among the factors that may be considered are the financial condition of the depositories, including their credit standing, and the nature of their operations.

**Risk Management:  
Customers**

**Risk Assessment of Customers**

*A broker/intermediary should assess the risks of doing business with a customer and should regularly monitor such risks throughout the term of the relationship with the customer.*

- 32 A broker/intermediary, prior to establishing a relationship with a customer, should assess the risks of doing business with that customer and should regularly monitor these risks throughout the term of the relationship with the customer. In general, a broker/intermediary's consideration should focus on the following areas:
  - (a) the nature of the customer (e.g., institutional or retail) and its corresponding level of experience and sophistication;
  - (b) the creditworthiness of the customer, as measured by established credit policies and procedures of the broker/intermediary; and
  - (c) the authority (including apparent authority) of the customer to conduct its proposed trading activities, including the customer's legal authority and the capacity of the individuals responsible for the trading.
- 33 Review of customers' financial condition, and related decisions with respect to customers, should be conducted by persons and business units within the broker/intermediary (a) that are independent of the sales personnel, and (b) whose compensation is not directly related to the volume or profitability of trading conducted by customers.
- 34 Customer margin requirements and, where appropriate, position limits should be established at levels that are adequate, in the judgment of the broker/intermediary, to protect the broker/intermediary against reasonably foreseeable risks arising from the customer's trading activities. Customers' significant market exposures should be reviewed on at least a daily basis and, where necessary for the protection of the broker/intermediary, the broker/intermediary should call for additional collateral, modify margin requirements or position limits, require customers to reduce the size of existing positions or take other appropriate actions.



35 Brokers/intermediaries should establish and enforce policies and procedures regarding the prompt collection of customer margin (other than in the case where there are appropriate credit arrangements in place) and the liquidation of customer accounts (or other appropriate action) where necessary.

36 Brokers/intermediaries should establish and enforce procedures regarding account opening and trading by omnibus and introduced accounts, recognizing the potential exposure to the broker/intermediary that may arise from such accounts.

37 Brokers/intermediaries should establish risk management procedures for trading by affiliates carried on their books. Such procedures should include, among others, position limits for affiliates' trading activities based on their financial status.

**Legal Relationships with Customers**

38 Brokers/intermediaries should prepare and utilize written agreements with their customers that clearly delineate the respective rights and obligations of the brokers/intermediaries and their customers. Such agreements should provide a basis for allocating between brokers/intermediaries and their customers responsibility for all material aspects of their relationships and risk exposures and should take into account the particular requirements of each customer and its relationship with the broker/intermediary.

39 A broker/intermediary should provide its customers, upon request, with information regarding the financial status of the broker/intermediary (subject to appropriate confidentiality considerations) and the identities of depositories and clearing brokers utilized by the broker/intermediary.

40 In general, where a customer seeks to obtain beneficial treatment for positions held for hedging, arbitrage or other purposes, a broker/intermediary should be able to rely on representations provided by its customer that the positions are eligible for such treatment. A broker/intermediary should establish and enforce procedures, however, to deal with those situations in which the broker/intermediary forms a judgment (based on information known to the broker/intermediary) that such representations are not accurate. Such policies or procedures might include making appropriate inquiries of the customer's senior management or requiring the customer to provide documentation to support its representations.

**Protection of Customer Property; Financing of Customer Margin**

41 Brokers/intermediaries should establish and enforce appropriate policies and procedures, taking into account applicable laws and regulations, to identify and protect customer property in their custody or control. Such policies and procedures might include segregation or other separation of customer property from proprietary property, maintenance of appropriate books and records identifying customer property, maintenance of adequate capital, and/or restrictions on the investment or other use of customer property.

*Brokers/intermediaries should prepare and utilize written agreements with their customers that clearly delineate the respective rights and obligations of the brokers/intermediaries and their customers.*

42



- 42 Except where appropriate and legally permissible credit arrangements have previously been established, brokers/intermediaries should promptly collect margin from their customers. In those instances in which margin is not collected within a reasonable period of time, appropriate adjustments, which may include requirements for financial reserves or additional collateral, should be imposed to reflect the potential exposure of brokers/intermediaries to their customers. The adequacy of these arrangements should be regularly re-evaluated in light of changing market conditions and should be adjusted as necessary.

### **Risk Management: Internal Controls**

---

*A broker/intermediary engaging in customer and proprietary trading should establish and enforce appropriate policies and procedures to identify customer property and to protect it against risks arising as a result of its proprietary trading activities.*

- 43 A broker/intermediary engaging in customer and proprietary trading should establish and enforce appropriate policies and procedures to identify customer property and to protect it against risks arising as a result of its proprietary trading activities. Such policies and procedures should include the maintenance of appropriate books and records that, among other things, separately identify customer and proprietary accounts and active monitoring of proprietary trading activities, including, if appropriate, the establishment of risk-based position limits.
- 44 Brokers/intermediaries should conduct regular internal reviews of their customer and proprietary accounts, including recordkeeping and other account maintenance matters, to monitor the broker/intermediary's compliance with applicable laws and regulations and internal policies and procedures. Such reviews should be conducted by personnel who are independent of proprietary traders and personnel responsible for customer relationships.
- 45 The Board of Directors or senior management of a broker/intermediary should establish general risk management guidelines and procedures for proprietary trading activities of the broker/intermediary, including instruments and strategies, position and trading limits for trading desks, business units and/or individual traders, periodic stress testing and cash flow and "value at risk" analyses. Compliance with such procedures and limits should be monitored regularly by personnel independent of proprietary traders. The Board of Directors or senior management should periodically review and modify such guidelines and policies, as necessary or appropriate.
- 46 Adequate separations should be imposed between (a) back office personnel responsible for trade reconciliation, margin, position limits, preparation and maintenance of books and records and other similar matters as well as compliance personnel, risk management personnel and treasury or funding personnel, and (b) personnel responsible for customer relationships or proprietary trading. The authority of appropriate personnel in these areas should be clearly established.



## Recommendations For Customers

### Legal Relationships with Brokers/Intermediaries

47 Customers should implement and enforce policies and procedures that are appropriate in the context of their businesses and the nature and level of their trading activities, (1) regarding the establishment of relationships with brokers/intermediaries, including specific criteria for the selection of brokers/intermediaries and the designation of personnel with the authority to negotiate, approve and execute agreements with brokers/intermediaries, and (2) ensuring that personnel with responsibility for reviewing and approving agreements, and monitoring relationships with brokers/intermediaries, are independent of the customer's trading personnel.

48 Customers should ensure that they understand the risks of their trading activities, the nature of their legal relationships with their brokers/intermediaries and the risks of utilizing their brokers/intermediaries and of trading on specific exchanges/clearinghouses (including an understanding of applicable laws and regulations of relevant jurisdictions). Customers should also ensure that they understand the nature of each broker/intermediary's legal relationships with relevant exchanges/clearinghouses, clearing brokers and depositories, and the risks to the customer arising from such relationships.

49 Customers should consider whether the following issues are addressed in each written agreement with a broker/intermediary and should, in establishing credit and/or position limits with each such broker/intermediary, take into account the manner in which such issues are dealt with in such agreement: (1) the broker/intermediary's right to close out the customer's account and liquidate positions, and the notice periods required for such actions; (2) the broker/intermediary's right to collect margin in excess of exchange/clearinghouse requirements; (3) the customer's right to withdraw excess margin; (4) the management of customer property held by the broker/intermediary; (5) the customer's exposure to the failure of exchanges/clearinghouses; (6) the customer's exposure to the failure of clearing brokers selected by the broker/intermediary; and (7) the customer's exposure to the failure of depositories holding customer property.

### Risk Assessment of Brokers/Intermediaries

50 Customers should consider, based on the terms of their agreements with their brokers/intermediaries and the allocation of responsibilities in such agreements, the credit and other material risks arising from the execution and/or clearing of transactions through such brokers/intermediaries.



**51** The primary factors to be considered with respect to each broker/intermediary should include, among others, its credit standing, capital and financial condition, the exchanges/clearinghouses of which the broker/intermediary is a member, the type of firm (for example, a bank, securities broker, insurance company or an affiliate thereof), and whether or not it engages in trading for its own account and/or carries accounts for its affiliates. Other factors that might also be considered, depending on the size and nature of the customer's trading activities and the extent of the customer's use of the broker/intermediary, include the broker/intermediary's management experience and capabilities, operational capacity, risk management systems and disaster recovery procedures.

**52** As part of its evaluation of its brokers/intermediaries, a customer should be aware of and consider the risk arising from the potential default of the broker/intermediary as a result of (a) the trading activities of the broker/intermediary or its affiliates, (b) the trading activities of other customers of the broker/intermediary (and customers should, in this connection, consider the procedures used by the broker/intermediary in establishing customer accounts and in the monitoring and management of credit and other risks arising from its carrying of such accounts), and (c) the default of a clearing broker or depository utilized by the broker/intermediary.

---

*Customers should consider information available about the risks of trading on particular exchanges/clearinghouses, prior to executing trades on such markets.*

**53** Based on its consideration of the credit risk arising from the execution and/or clearing of transactions through a particular broker/intermediary, a customer may wish to consider obtaining from the broker/intermediary a form of credit enhancement, such as an affiliate guarantee or the guarantee (or letter of credit) of a third party. If a customer relies on such forms of credit enhancement, it should ensure that the terms and scope of such credit enhancement are understood by and acceptable to the customer and that the credit enhancement is legally enforceable.

### **Risk Assessment of Exchanges/Clearinghouses**

**54** Customers should consider information available about the risks of trading on particular exchanges/clearinghouses, prior to executing trades on such markets. Such risks should also be considered on an ongoing basis.

45



55 Among the factors that might be appropriate to consider in determining whether to transact on a particular exchange/clearinghouse are the quality of the regulatory and oversight system of the exchange/clearinghouse, the applicable financial integrity system, relevant customer protection mechanisms (e.g., segregation requirements, account insurance, guarantees or compensation funds), the extent to which the exchange/clearinghouse has the right to force the liquidation of customer positions, the source and liquidity of relevant financial support, the margining and settlement system (including the variation margin settlement periods and the extent to which variation margin is paid out to customers), the ability to transfer positions and property in the event of a default, other operational issues and the applicable legal and regulatory system, including applicable bankruptcy laws.

### Internal Risk Management Procedures

*The Board of Directors or senior management of a customer should, in the manner and to the extent appropriate, understand its proposed trading activities and establish general risk management guidelines and procedures for such activities.*

56 The Board of Directors or senior management of a customer should, in the manner and to the extent appropriate in the context of its business and the nature and level of its trading activities, understand its proposed trading activities and establish general risk management guidelines and procedures for such activities, including instruments and strategies, position and trading limits for trading desks, business units and/or individual traders, receipt of confirmations and other appropriate documents, periodic stress testing and cash flow analysis and determination of "value at risk". Compliance with such procedures and limits should be monitored on a regular (and, where appropriate, daily) basis by personnel independent of trading personnel. The Board of Directors or senior management should periodically review and modify such guidelines and policies, as necessary or appropriate.

57 A customer should, in the manner and to the extent appropriate in the context of its business and the nature and level of its trading activities (1) establish and enforce policies and procedures to review, on a regular basis, market, credit, operational and other risks arising from its trading activities, including daily reconciliation of trades, margin requirements and open positions and monitoring of hedging or arbitrage positions, (2) ensure that such functions are performed by personnel independent of trading personnel, and (3) ensure that internal reviews of compliance with such policies and procedures should also generally be conducted by personnel independent of trading personnel.

58 Adequate separations should be imposed between (a) back office personnel responsible for trade reconciliation, margin, preparation and maintenance of books and records and other similar matters, as well as compliance personnel, risk management personnel and treasury or funding personnel, and (b) personnel responsible for the customer's trading activities. The authority of appropriate personnel in these areas should be clearly established.

- 59 Customers should establish appropriate credit and/or position limits for each broker/intermediary, based on their credit assessment of the broker/intermediary. Credit exposure to each broker/intermediary should, where warranted and feasible in light of the size and nature of the customer's business and the level of its trading activities, be monitored regularly by personnel independent of trading personnel. Customers should establish procedures for managing excess margin held by brokers/intermediaries.
- 60 Those customers with substantial exposure to brokers/intermediaries as a result of the customers' trading activities should establish and maintain back-up clearing relationships with brokers/intermediaries to be utilized in emergency situations. Such relationships should include completed contractual arrangements with such back-up brokers/intermediaries and periodic testing of procedures for transfers of positions and property and continuation of trading.

**The Futures Industry Association** is a U.S.-based international association which acts as a principal spokesman for the futures and options industry. Our membership, which has its roots in the brokerage community, now represents all facets of the futures industry including institutional users doing business internationally. FIA actively works to preserve the system of free and competitive markets by representing the interests of the industry in connection with legislative and regulatory issues.

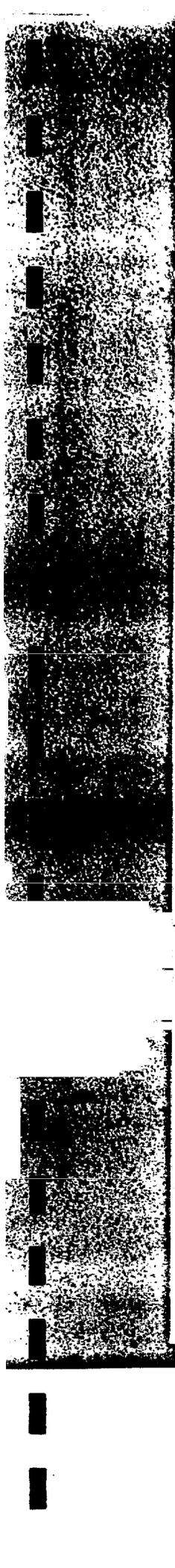
For additional copies of the FIA Task Force Recommendations, phone (202) 466-5460, fax: (202) 296-3184.



# **SiPC and Customer Protection**

**SECURITIES INVESTOR PROTECTION CORPORATION**

---



# **SIPC** and **Customer Protection**

SECURITIES INVESTOR PROTECTION CORPORATION  
805 FIFTEENTH STREET, N.W., SUITE 800  
WASHINGTON, D.C. 20005-2207

© 1992 Securities Investor Protection Corporation

---

# Preface

This booklet describes in some detail the implementation of the Securities Investor Protection Act of 1970 as amended (SIPA), and offers a brief account of its history and purpose.

SIPA protects customers of securities broker-dealers, thereby promoting confidence in United States securities markets. The organization charged with its administration, the Securities Investor Protection Corporation (SIPC), is a private, non-profit, membership corporation financed by the securities industry, and with close ties to the federal government. SIPC provides the financial protection afforded by the law to customers of members that fail.

SIPC's organization and customer protection procedures are summarized in these pages. New interpretations, administrative decisions, and further amendments, however, make any description of SIPA subject to change. Although this booklet is revised periodically to take such changes into account, it should not be considered a definitive interpretation of SIPA.

April, 1992  
Third Edition



Public Law 91-598  
91st Congress, H. R. 19333  
December 30, 1970

## An Act

84 STAT. 1636

To provide greater protection for customers of registered brokers and dealers and members of national securities exchanges.

*Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,*

### SECTION 1. SHORT TITLE, ETC.

(a) SHORT TITLE; TABLE OF CONTENTS.—This Act, with the following table of contents, may be cited as the "Securities Investor Protection Act of 1970".

Securities In-  
vestor Protec-  
tion Act of  
1970.

# Contents

I. INCEPTION AND ORGANIZATION . . . . .	1
Legislative History . . . . .	1
"Paperwork Crunch" . . . . .	1
Industry Program . . . . .	1
Joint Proposal . . . . .	1
1978 Amendments . . . . .	2
The Corporation . . . . .	2
Membership . . . . .	2
Entire Community of Broker-Dealer Customers . . . . .	2
Government, Industry, and Public Directors . . . . .	3
Corporate Powers . . . . .	3
Securities and Exchange Commission Oversight . . . . .	3
Rules and Bylaws . . . . .	3
Enforcement, Examinations, and Reports . . . . .	4
The SIPC Fund . . . . .	4
Assessments . . . . .	4
Statutory Fund Levels . . . . .	4
Assessment History . . . . .	5
Collection and Penalties . . . . .	5
Voluntary Contributions . . . . .	5
Borrowing and Lines of Credit . . . . .	5
Investment Income . . . . .	6
II. MONITORING MEMBER FINANCIAL CONDITION AND INITIATING PROCEEDINGS . . . . .	7
Self-Regulators Examine SIPC Members . . . . .	7
Notice of Member Financial Difficulty . . . . .	7
Most Members Correct Difficulties . . . . .	7
Determining Failure . . . . .	8
Customer Protection Proceedings . . . . .	8
Three Alternatives . . . . .	8
Applying For Trustee Appointment . . . . .	8
SIPC Specifies Trustee, Counsel . . . . .	9
Court Powers and Duties . . . . .	9
Nature of a SIPC Proceeding . . . . .	9
Trustee's Powers and Duties . . . . .	9
Blending of SIPA with Bankruptcy Code . . . . .	10

III. CUSTOMER PROTECTION . . . . . 11

- “Customer” Defined . . . . . 11
- Protected Property . . . . . 11
- Transfer of Customer Accounts . . . . . 11
- Satisfaction of Customer Claims . . . . . 11
- Direct Payment Procedure . . . . . 14
- Advances to Satisfy Customer Claims . . . . . 14
- Advances for Administration . . . . . 14
  - SIPC’s Subrogation and Recoupment Rights . . . . . 14
  - Open Contractual Commitments . . . . . 15
- Assistance in Investigations . . . . . 15

IV. INVESTOR PROTECTION IN PERSPECTIVE . . . . . 16

- Member Identification . . . . . 16
- Improved Investor Protection . . . . . 16

# Inception and Organization

## LEGISLATIVE HISTORY

The Securities Investor Protection Corporation (SIPC) was created by the Securities Investor Protection Act of 1970 (SIPA), a federal statute effective December 30, 1970. As discussed below, SIPA was enacted to address a potential threat to the viability of our securities markets.

In passing SIPA, Congress' objective was to protect—up to certain defined limits—the customers of failed broker-dealers against loss of cash and securities. While protecting customers, SIPA's provisions for completion of open contractual commitments between broker-dealers limit the economic impact of failure on the brokerage community.

The Chandler Act (1938) was the first legislation recognizing the unique problems of a bankrupt broker-dealer's customers.<sup>1</sup> An amendment to the Bankruptcy Act, that legislation addressed the priorities between a bankrupt broker-dealer's customers and other creditors.

### "Paperwork Crunch"

There was little reason to question this legislation's adequacy until the emergence of operational and financial problems created by the "paperwork crunch" and a declining market in the late 1960's. During that period, hundreds of broker-dealers merged, were acquired, or simply went out of business. Some were unable to meet their obligations to customers and went bankrupt.

In early 1970, several versions of a proposed statute for the protection of customers were under consideration in Congress. A broad-based securities industry committee was formed to develop an industry-wide customer protection plan.<sup>2</sup>

<sup>1</sup>11 U.S.C. §96 (repealed, 1978) (originally enacted as Act of June 22, 1938, c.575, §1, 52 Stat. 869).

<sup>2</sup>A letter to that effect, dated April 14, 1970, was sent to the Chairman of the Securities and Exchange Commission and Congressional leaders.

## Industry Program

A five point program unanimously endorsed by the industry committee recommended:

*Expansion of the protection available to all customers<sup>3</sup> for their funds and securities held by broker-dealers;*

*Development of a program consistent with the established public policy of self-regulation in the securities industry;*

*That the particular needs and circumstances of each industry organization be reflected;*

*Establishment of an equitable formula of financing such a program—equitable in terms of both the size and nature of the risk involved;*

*Presentation to the Securities and Exchange Commission (SEC) and Congress of a unified and constructive approach by the entire securities industry.*

Within the existing fabric of self-regulation, the committee contemplated a plan to protect public customers of broker-dealers up to certain defined limits. The plan would maintain public confidence in the nation's securities markets by assuring payments to public customers "without at the same time creating a vast new governmental agency in this highly specialized area."<sup>4</sup>

## Joint Proposal

Representatives of the securities industry, the Federal Reserve Board, Office of Management and Budget, the Department of the Treasury, and the SEC conferred on draft bills proposed by the industry group and the SEC staff. Their joint proposal would have created an organization performing a role in the secu-

<sup>3</sup>Although trust funds had been created by several exchanges for the protection of customers of member firms experiencing financial difficulty, there was no fund or machinery in existence for the protection of customers on an industry-wide basis.

<sup>4</sup>Hearings on H.R. 13308, H.R. 17585, H.R. 18081, H.R. 18109, H.R. 18458 Before the Subcomm. on Commerce and Finance of the House Comm. on Interstate and Foreign Commerce, 91st Cong. 2d Sess. 169 (1970) (Testimony of Ralph D. DeNunzio, Chairman, Joint Securities Industry Task Force).

rities industry somewhat similar to those established to insure depositors in banks, savings and loan associations, and credit unions; that is, the Federal Deposit Insurance Corporation (FDIC), Federal Savings and Loan Insurance Corporation (FSLIC), and National Credit Union Administration (NCUA).

Although, the general pattern recommended by the industry task force was retained, the product which finally emerged from the House and Senate conference differed in many respects from earlier versions. The SEC's powers regarding financial responsibility of securities broker-dealers were broadened, while the industry's existing self-regulatory structure was retained. SIPA neither created a new regulatory organization nor an additional layer of regulatory authority. The Bankruptcy Act was not amended; rather, special liquidation procedures for broker-dealers were adopted.

#### 1978 Amendments

A few years' experience with SIPA suggested some changes were in order. Prescribed procedures were in some respects inefficient, inflexible, and not the most expedient. Customer claims were often "satisfied" by cash payments in lieu of securities due them.

In late 1973, a special task force studied the matter and made recommendations to SIPC's Board of Directors. Most were adopted, translated into legislative form, and transmitted to Congress. In May 1978, they became law as the "Securities Investor Protection Act Amendments of 1978."

The amendments were designed to increase customer protection, speed up the liquidation process, and reduce costs. Their provisions are incorporated in the explanation of SIPA which follows.<sup>5</sup>

## THE CORPORATION

SIPC is a nonprofit, membership corporation subject to, and with the powers conferred upon a non-profit corporation by the District

<sup>5</sup>For an analysis of the ways in which the amendments changed the original 1970 Act, see "Securities Investor Protection Act Amendments of 1977" (sic) Report No. 95-746. Report to the Committee on Interstate and Foreign Commerce of the House of Representatives.

of Columbia Nonprofit Corporation Act, except where that is inconsistent with the provisions of SIPA.<sup>6</sup> The Corporation is to exist until dissolved by Act of Congress and with limited exceptions is exempt from federal or local taxation. Though subject to SEC and Congressional oversight, SIPC is not an agency or establishment of the United States Government.

#### Membership

SIPC membership is composed of all persons registered as brokers or dealers under Section 15(b) of the Securities Exchange Act of 1934 (1934 Act) and all members of a national securities exchange except:<sup>7</sup>

1. Those whose principal business in SIPC's determination is conducted outside the United States, its possessions and territories;<sup>8</sup> and
2. Persons whose business as a broker or dealer consists exclusively of the:
  - a. distribution of shares of registered open end investment companies or unit investment trusts,
  - b. sale of variable annuities,
  - c. business of insurance, or
  - d. business of rendering investment advisory services to one or more registered investment companies or insurance company separate accounts.

Broker-dealers excluded from SIPC membership because of the nature of their business are required to notify SIPC, indicating the basis for exclusion. If the character of the business changes, SIPC requires written notice to this effect.

#### Entire Community of Broker-Dealer Customers

During Congressional hearings and debates leading to SIPA's passage, considerable discussion focused on standards or requirements to be met by broker-dealers to become SIPC members. The Senate bill, indeed, had been amended to include such standards.

<sup>6</sup>Section 3(a).

<sup>7</sup>Sections 3(a)(2)(A) and 16(12).

<sup>8</sup>Section 3(a)(2)(C) provides that members so excluded "may become members of SIPC under such conditions and upon such terms as SIPC shall require by rule, taking into account such matters as the availability of assets and the ability to conduct a liquidation if necessary."

Many, however, felt such requirements could defeat the objective of protecting the entire community of broker-dealer customers. During Congressional hearings, Hamer H. Budge, then Chairman of the SEC, argued that when the FDIC was established, some banks were not permitted to become members because of their financial condition. To exclude the brokerage firms that might be in the same category as those banks, Mr. Budge said, would not be in the public interest. He explained:

*"The purpose of the legislation is to protect the customers of the brokerage houses, and if we take out the firms where the greatest exposure is, we are removing the protection of all the customers of those firms. It isn't as easy to determine the financial condition of a brokerage house as it is a bank and savings and loan. The financial condition can change radically very quickly, much more so than a bank or savings and loan."*<sup>9</sup>

Although membership standards were deleted from the final bill, Congress addressed the need to upgrade broker-dealer financial responsibility. Such upgrading, Congress decided, could best be accomplished by granting the SEC increased authority, rather than by legislation. Section 11(d) of SIPA provided the SEC authority to achieve that objective and it, in turn, promulgated Rule 15c3-3, the customer protection rule, effective January 15, 1973. (17 CFR 240.15c3-3).

#### **Government, Industry, and Public Directors**

SIPA established a board of seven directors to determine SIPC's policies and govern its operations.<sup>10</sup> The Secretary of the Treasury and Federal Reserve Board each appoint a director selected from their respective officers and employees. Five directors are appointed by the President of the United States, with the advice and consent of the Senate, as follows:

a. three from among persons associated with, and representative of, different aspects of the securities industry, not all of

whom are from the same geographical area;

b. two from among persons in the general public who are not associated with any broker or dealer, a national securities exchange or other securities industry group and who have not had any such association during the two years preceding appointment.

The President designates the Chairman and Vice Chairman from the public directors. Directors are appointed for a term of three years. The Chairman is SIPC's chief executive officer.

#### **Corporate Powers**

In addition to the general corporate powers of a nonprofit corporation, SIPC has certain other powers necessary to accomplish its purpose. It is authorized to establish the SIPC Fund, collect assessments, and, if necessary, borrow monies.<sup>11</sup> SIPC is empowered to apply for appointment of trustees, including itself or a SIPC employee; assist in the liquidation of failed members;<sup>12</sup> pay customers directly in certain circumstances;<sup>12a</sup> and consult and cooperate with self-regulatory organizations on inspections and reports concerning SIPC members.<sup>13</sup>

The Board of Directors can adopt, amend, or repeal bylaws regarding its business and rules defining terms in SIPA, undefined therein, and procedures for liquidations and direct payments to customers. As discussed below, SIPC bylaws and rules require SEC approval.

#### **Securities and Exchange Commission Oversight**

##### *Rules and Bylaws*

SIPC's Board files with the SEC any proposed rule, amendment to, or repeal of a rule (collectively referred to hereafter as "rule change"). The SEC then publishes a descriptive notice of the rule change, allowing interested parties to submit their views. Within 35 days after the notice's publication, or up to 90 days when appropriate, the SEC must either approve or order proceedings to determine

<sup>9</sup>Hearing on H.R. 13308, H.R. 17585, H.R. 18081, H.R. 18109, H.R. 18458 Before the Subcomm. on Commerce and Finance of the House Comm. on Interstate and Foreign Commerce, 91st Cong., 2d Sess. 367-68 (1970).

<sup>10</sup>Section 3(c).

<sup>11</sup>Sections 4(f), (g), and (h).

<sup>12</sup>Sections 5, 6, 7, 8, and 9.

<sup>12a</sup>Section 10.

<sup>13</sup>Section 13.

55

whether the proposed rule change should be disapproved.<sup>14</sup>

Similarly, any proposed bylaw, amendment to, or repeal of a bylaw must also be filed with the SEC. Each proposed bylaw or change takes effect thirty days after filing unless the SEC disapproves it as contrary to the public interest, or finds a matter of such significant public interest that it be treated as if a rule.

Finally, the SEC may require SIPC to adopt, amend, or repeal any SIPC bylaw or rule, if it determines such action to be in the public interest or necessary to carry out SIPA's purposes.

#### *Enforcement, Examinations, and Reports*

If SIPC should refuse to commit its funds or otherwise act for the protection of any member's customers, the SEC may apply to the United States district court in which SIPC's principal office is located for an order requiring SIPC to discharge its obligations under SIPA and for such other relief the court may deem appropriate to carry out SIPA's purposes.

The SEC may examine and inspect SIPC and require it to furnish reports and records. As soon as practicable after the close of each fiscal year, SIPC submits to the SEC a written report covering its business and exercise of authority during the year. The report must include financial statements examined and reported on by independent public accountants. The SEC, in turn, transmits the annual report to the President and Congress with appropriate comments.

## THE SIPC FUND

The SIPC Fund consists of the aggregate of cash on hand or on deposit, amounts invested in United States Government or agency securities, and certain confirmed lines of credit defined by SIPA.<sup>15</sup> The Fund's principal sources of revenues are described below.

<sup>14</sup>Sections 3(e)(2)(C) and (D) describe grounds for approval or disapproval of proposed rule change. Section 4(e)(D) describes two exceptions to these usual procedures.

<sup>15</sup>Section 4(a).

## Assessments

From December 30, 1970, to June 30, 1978, SIPC's principal source of revenue was assessments upon its members. SIPA provides two phases of assessments: one to build the SIPC Fund and another to maintain it.

The build-up phase encompassed that period required for the SIPC Fund to reach \$150 million—a level attained in 1977. During the build-up, an initial assessment of  $\frac{1}{8}$  of 1 percent of members' 1969 gross revenues from the securities business payable early in 1971 and a general assessment payable quarterly at  $\frac{1}{2}$  of 1 percent of such revenues for 1971 through 1977 were collected.<sup>16</sup>

## Statutory Fund Levels

Once the build-up phase was completed, the maintenance phase provisions applied. During any period in which the Fund is less than \$100 million,<sup>17</sup> or there is outstanding borrowing by SIPC, the assessment is at the rate of no less than  $\frac{1}{2}$  of 1 percent of the gross revenues of each member. Assessments may be set at a rate between  $\frac{1}{2}$  and 1 percent if SIPC determines after consulting the self-regulatory organizations that such rate will have no material adverse effect on the financial condition of its members or their customers. When the Fund is between \$100 and \$150 million<sup>18</sup> (exclusive of lines of credit) and there is no outstanding borrowing, aggregate assessments are not to be less than  $\frac{1}{4}$  of 1 percent per annum of members' aggregate gross revenues from the securities business.<sup>19</sup> When the Fund exceeds \$150 million,<sup>20</sup> SIPC is empowered to impose such assessments as it deems necessary and appropriate to maintain the Fund, except that the rate may not exceed in the aggregate one percent of a member's gross revenues from the securities business.<sup>21</sup>

<sup>16</sup>Section 4(d)(1).

<sup>17</sup>Or such other amount as the SEC may determine in the public interest.

<sup>18</sup>See note 17 above.

<sup>19</sup>Section 4(d)(1)(B)(11).

<sup>20</sup>See note 17 above.

<sup>21</sup>Section 4(c)(2) grants SIPC the authority to vary assessments between classes of members based on a number of economic factors. The authority has not been used.

### Assessment History

Following attainment of the \$150 million Fund level, SIPC reduced the assessment rate from  $\frac{1}{2}$  of 1 percent to  $\frac{1}{4}$  of 1 percent during the first six months of 1978. Assessments were suspended for the remainder of that year.

In 1979 a uniform assessment of \$25 for each SIPC member went into effect. In 1983, the Fund decreased to below \$150 million and, as required by SIPA, assessments at the rate of  $\frac{1}{4}$  of 1 percent, with a minimum annual assessment of \$25, were reimposed.

On March 31, 1986, assessment at  $\frac{1}{4}$  of 1 percent was discontinued and a uniform annual assessment of \$100 for each SIPC member went into effect. The statute authorizes SIPC to impose a minimum annual assessment not greater than \$150 per member. In January 1989, an assessment at  $\frac{3}{16}$  of 1 percent, with a minimum of \$150, was imposed.

On September 26, 1991, SIPC's Board of Directors adopted amendments to the SIPC bylaws regarding the size of SIPC Fund and the assessment base and rate. The Board directed that the SIPC Fund should be built to \$1 billion and that the Fund should grow at the rate of 10% per year. The Board also directed that the base of assessment be changed from "gross revenues from the securities business" to "net operating revenues." The amended bylaw provides that SIPC, in November of each year, shall project future expenses as well as income together with other relevant data to arrive at the assessment rate. That rate for fiscal years beginning in 1991, and ending not later than December 31, 1992, will be .00065, which is considerably below the 1990 rate of .001875. The minimum assessment of \$150 per year or for any part of a year will remain unchanged.

SIPC bylaw provides for the automatic imposition of assessments at the rate of  $\frac{1}{8}$  of 1 percent when the Fund totals, or the SIPC Board determines it is "reasonably likely" to total, less than \$250 million.

### Collection and Penalties

SIPC assessments are collected by the self-regulatory organization which has the responsibility to examine the member for compliance with applicable financial responsibility rules.

Failure to pay assessments when due results in the imposition of interest<sup>22</sup> and continued delinquency after notice results in being unlawful for the member to engage in business as a broker-dealer.<sup>23</sup>

### Voluntary Contributions

Any funds held by a trust established by a self-regulatory organization prior to January 1, 1970, may be contributed and transferred to SIPC. Under this provision of SIPA, SIPC received \$3,011,925 during 1971 from the trust fund of the American Stock Exchange, Inc., members of which received a reduction in SIPC assessments during the years 1974-1976 to reflect that contribution.

### Borrowing and Lines of Credit

SIPC may borrow from banks or other financial institutions pursuant to lines of credit or other written agreements.<sup>24</sup> In the event the SIPC Fund should prove inadequate, presumably resulting only from a crisis of great severity and magnitude, SIPC may, through the SEC, borrow up to \$1 billion from the U.S. Government. The SEC would finance such a loan through the issuance of notes or other obligations to the Secretary of the Treasury, who would set their terms and conditions.

Should such a loan become necessary, SIPA requires SIPC to submit a plan to the SEC assuring repayment as promptly as feasible under the circumstances.<sup>25</sup>

A \$65 million credit agreement with a group of banks was entered into on April 14, 1971. This line of credit, which was not used,

<sup>22</sup>If all or any part of an assessment payable under Section 4 of the Act has not been received by the collection agent within 15 days after the due date thereof, the member shall pay, in addition to the amount of the assessment, interest at the rate of 20% per annum on the unpaid portion of the assessment for each day it has been overdue. If any broker or dealer has incorrectly filed a claim for exclusion from membership in the Corporation, such broker or dealer shall pay, in addition to assessments due, interest at the rate of 20% per annum on the unpaid assessment for each day it has not been paid since the date on which it should have been paid.

<sup>23</sup>Section 14(a).

<sup>24</sup>Sections 4(a)(3) and (4), and 4(f).

<sup>25</sup>If the SEC questions SIPC's ability to repay such loans through assessments pursuant to such a plan, Section 4(g) empowers the SEC to impose a fee on the purchasers of equity securities that would apply to transactions in excess of \$5,000.

was reduced by \$10 million on April 1, 1972, and by the same amount on April 1 of the succeeding four years, with a final balance of \$15 million expiring on October 13, 1976. Given the significant build-up of the Fund by mid-1975, SIPC terminated the credit agreement on September 19, 1975.

On April 1, 1986, in conjunction with the termination of assessments based on a percentage of gross revenues, SIPC entered into a \$500 million line of credit agreement with a

group of banks. On April 1, 1989, this line of credit was renewed. On April 1, 1992, SIPC established a \$1 billion revolving line of credit with a group of banks.

#### **Investment Income**

Revenue from investments in United States Government and agency securities are SIPC's principal source of revenue in addition to assessments.

# Monitoring Member Financial Condition And Initiating Proceedings

## SELF-REGULATORS EXAMINE SIPC MEMBERS

SIPA's Section 13 was designed to upgrade the financial practices and responsibility of securities industry members over a period of time.<sup>26</sup>

The self-regulatory organizations (SROs) inspect or examine SIPC members under their jurisdiction for compliance with financial responsibility rules. When a SIPC member broker-dealer is a member of more than one SRO, the SEC designates one of them, or itself, the examining authority. By bylaw or rule, SIPC can require reports of such examinations or inspections.

Improved broker-dealer operations and the combination of more stringent requirements for entering the securities business, new financial responsibility rules, and noticeable improvement in monitoring broker-dealer financial condition by the SEC and SROs since SIPC's inception contributed to a sharp decline in the number of customer protection proceedings commenced in the late 1970s.

### Notice of Member Financial Difficulty

Section 5(a)(1) of SIPA requires the SEC and SROs to notify SIPC immediately after discovering a broker-dealer subject to their

<sup>26</sup>Subsection (e) of Section 13 specifies that "SIPC shall consult and cooperate with the self-regulatory organizations toward the end:

(1) that there may be developed and carried into effect procedures reasonably designed to detect approaching financial difficulty upon the part of any member of SIPC;

(2) that, as nearly as may be practicable, examinations to ascertain whether members of SIPC are in compliance with applicable financial responsibility rules will be conducted by the self-regulatory organizations under appropriate standards (both as to method and scope) and reports of such examinations will, where appropriate, be standard in form; and

(3) that, as frequently as may be practicable under the circumstances, each member of SIPC will file financial information with, and be examined by, the self-regulatory organization which is the examining authority for such member."

regulation is in or approaching financial difficulty. The notice—known as a "5(a) referral"—is to afford SIPC ample time to prepare for selection of a trustee and supporting personnel capable of handling a particular case's problems and prepare to satisfy customer claims.

No specific guidelines for determining "financial difficulty" have been established. There are differences in the various reporting and surveillance systems and subjective factors are always present. In view of the number of self-regulatory organizations involved and differences in their rules, procedures and problems, SIPC relies on the judgment and experience of their examining staffs, and the SEC, to determine the circumstances under which a 5(a) referral is given.<sup>27</sup> Experience to date has confirmed that this decision was correct.

After a 5(a) referral is received, SIPC reviews the facts furnished and consults with the examining authority regarding additional data, such as results of examinations and current financial reports. Communications continue until the member corrects its difficulties or the determination is made that it must be liquidated.

### Most Members Correct Difficulties

The referral of a member under Section 5(a)(1) does not, of course, mean it is destined to be liquidated. The great majority of members so referred correct their financial difficulties.

Members may also reduce or terminate their businesses. A self-regulatory organization may assist and/or oversee such business reduction or self-liquidation without being deemed to have assumed any of the member's obligations.<sup>28</sup> SRO participation in a self-

<sup>27</sup>These notifications and the information on which they are based are not made public by SIPC when received since to do so might make difficult, if not impossible, efforts to prevent failure of a member.

<sup>28</sup>Section 13(b) grants immunity to self-regulatory organizations for actions taken or omitted in good faith under Sections 5(a)(1) and (2).

liquidation does not preclude subsequent SIPC action.

Occasionally a member's financial position may deteriorate very rapidly—if customers fail to deliver securities, other broker-dealers fail to honor commitments, the market price of particular securities declines very sharply, or for other reasons. The time span from early warning to SIPC's entry may be relatively short.

As soon as a member in trouble is brought to SIPC's attention, it establishes a file, collects information from available sources, and determines whether or not, and to what extent, customers may be exposed. When a member's failure is imminent, SIPC determines which of three alternative customer protection proceedings is appropriate. The alternative procedures are described below.

### Determining Failure

SIPC determines a member has failed, or is in danger of failing, to meet its obligations to customers before initiating a proceeding. A member must meet one or more of four conditions specified in Section 5(b)(1) of SIPA. The member must be:

1. insolvent within the meaning of the Bankruptcy Code, or unable to meet its obligations as they mature;
2. the subject of a proceeding pending in any court or before any agency of the United States or any State in which a receiver, trustee, or liquidator for such debtor has been appointed;
3. not in compliance with applicable requirements under the 1934 Act or rules of the SEC or any self-regulatory organization with respect to financial responsibility or hypothecation of customers' securities; or
4. unable to make such computations as may be necessary to establish compliance with such financial responsibility or hypothecation rules.

## CUSTOMER PROTECTION PROCEEDINGS

### Three Alternatives

Once SIPC has determined that a member's customers require protection under SIPA, SIPC selects one of three alternative proceedings:

1. *Large cases.* If the member to be liquidated has 500 or more customers or obligations to general creditors and subordinated lenders of \$750,000 or more, a trustee other than SIPC or one of its employees must be designated by SIPC.

2. *Medium size cases.* If the member to be liquidated has fewer than 500 customers and obligations to general creditors and subordinated lenders are less than \$750,000, SIPC or a SIPC employee may be designated trustee at SIPC's discretion.

3. *Small cases.* SIPC may employ the Direct Payment Procedure if it determines that:

- a. the claims of all customers of the member aggregate less than \$250,000;
- b. the claim of each customer is within the limits of protection—\$500,000 per customer, no more than \$100,000 of which may be for cash; and
- c. the cost to SIPC of satisfying claims would be less than the cost of a court-supervised proceeding. In addition, either the member's broker-dealer registration must have been terminated or the member must have consented to SIPC's use of the Direct Payment Procedure.

The Direct Payment Procedure is described on page 14.

The first two alternatives differ only with respect to SIPC's option of designating itself or an employee trustee. They are alike in all other respects. Both are court-ordered and court-supervised liquidation proceedings.

If selection of a non-SIPC trustee is necessary, the position is filled from qualified candidates in the member's community. Generally, the non-SIPC trustee is an attorney, although other professionals have been named in some cases. To assist the trustee, SIPC seeks qualified local counsel to serve as trustee's counsel and, when necessary, a local accounting firm familiar with stock brokerage accounting.

### Applying for Trustee Appointment

In large and medium size cases (alternatives 1 and 2), SIPC applies to a federal district court for appointment of a trustee. In discharging its regulatory duties, the SEC usually seeks an injunction when it learns a broker-dealer is violating net capital or record

keeping rules or is engaged in other illegal conduct. SIPC usually applies to the court for appointment of a trustee at the same time.

It is not always possible, however, to determine whether there is a customer exposure prior to the SEC's court action. Accordingly, a restraining order is sometimes issued and a receiver appointed before SIPC is prepared to make the determination required by SIPA. In such cases, SIPC will later apply for a trustee's appointment if customer protection proves necessary.

In some instances, of course, SIPC action is unnecessary. A determination that the member, for example, had no public customers, had paid customers all amounts owed, or the difficulties had been remedied would obviate SIPC action.

#### **SIPC Specifies Trustee, Counsel**

If a member fails to contest successfully an application within three days after its filing, or such period as the court may order, the court issues a decree adjudicating that the member's customers are in need of protection under SIPA. The court then appoints a trustee for the liquidation of the member's business and as attorney for the trustee such persons as SIPC, in its sole discretion, specifies. No person may be appointed to either position if he or she is not "disinterested" within the meaning of Section 5(b)(6) of SIPA, SIPC is deemed by SIPA to be disinterested, as is a SIPC employee if, except for his or her employment by SIPC, he or she would meet the standards of disinterestedness set forth in the statute.<sup>29</sup>

If the member consents to SIPC's application, the court may make its adjudication and appoint a trustee immediately upon the filing of the application.

If the member contests SIPC's application, the court must hold a hearing within a short period of time, but usually no less than three business days after SIPC files its application. In view of a possible injection of new capital or other corrective action during that period, earlier court action might indeed be premature. Nevertheless, SIPC considers it important in many cases to end the member's access to customers' property and its assets, books and records. In such cases, SIPC urges ap-

<sup>29</sup>Section 5(b)(6).

pointment of a temporary receiver under Section 5(b)(2) to take control of assets pending the hearing.

#### **Court Powers and Duties**

Except as inconsistent with SIPA's provisions, the court is given the jurisdiction, powers, and duties conferred upon a federal court sitting in bankruptcy, together with other jurisdiction, powers, and duties prescribed by SIPA. Specifically, SIPA gives the court exclusive jurisdiction of: the failed member (debtor)<sup>30</sup> and its property, including property located outside the court's territorial limits and property held as security for a debt or subject to a lien; and of any suit against the trustee with respect to the liquidation proceedings.

SIPA also states the "court shall stay" pending proceedings to reorganize, conserve or liquidate the debtor or its property, and any other suit against any receiver, conservator, or trustee of the debtor or its property. In addition, the court may stay other actions involving the debtor or its property.

#### **Nature of a SIPC Proceeding**

SIPA sets forth the purposes of a proceeding in which a trustee has been appointed, the procedures to be followed, the powers and duties of the trustee, and the rights and priorities of the debtor's customers. The proceeding is essentially a liquidation and SIPA denominates it as such.

#### **Trustee's Powers and Duties**

The powers and duties of the trustee are quite broad. Section 7(a) gives the trustee the same powers and title with respect to the debtor and its property, and the same rights to avoid preferences as a trustee in bankruptcy.

In addition, the trustee may, with SIPC approval, hire, and fix the compensation of persons the trustee deems necessary for the liquidation proceeding and to margin and maintain the debtor's customer accounts for sale or transfer to another SIPC member.

<sup>30</sup>Section 16(5) of SIPA defines the term "debtor" (a term employed throughout Sections 6, 7, 8, 9, and 10) to mean the SIPC member in respect of whom an application has been filed or a Direct Payment Proceeding has been initiated.

The duties of the trustee, except where inconsistent with SIPA or as otherwise ordered by the court, are the same as the duties of a trustee in bankruptcy.

Though not required to, a trustee may reduce to money any securities constituting customer property or in the debtor's general estate. The trustee does have the duty to deliver to customers, to the maximum extent practicable, the securities and cash in their accounts as reflected therein on the filing date. The filing date is defined in Section 16(7).<sup>31</sup>

The trustee also has the duty, with SIPC's approval, to pay or guarantee loans collateralized by securities, providing the indebtedness does not appear to exceed the value of securities to be obtained thereby.

The trustee is obliged to conduct an investigation of debtor fraud, misconduct, mismanagement, irregularities, and any causes of action available to the estate. A report of the investigation must be made to SIPC and anyone else the court directs. The trustee must make reports to the court and to SIPC as prescribed by the Bankruptcy Code.

#### **Blending of SIPA with Bankruptcy Code**

The net effect of these provisions of SIPA is a blending of the statute with the provisions of the Bankruptcy Code dealing with ordinary bankruptcy. Such a blending was intended to provide the court and trustee with the flexibility necessary to properly conduct a complex proceeding.

<sup>31</sup>"Filing Date.—The term 'filing date' means the date on which an application for a protective decree is filed under section 5(a)(3), except that—

(A) if a petition under Title 11 of the United States Code concerning the debtor was filed before such date, the term 'filing date' means the date on which such petition was filed;

(B) if the debtor is the subject of a proceeding pending in any court or before any agency of the United States or any State in which a receiver, trustee, or liquidator for such debtor has been appointed and such proceeding was commenced before the date on which such application was filed the term 'filing date' means the date on which such proceeding was commenced; or

(C) if the debtor is the subject of a direct payment procedure or was the subject of a direct payment procedure discontinued by SIPC pursuant to section 10(f), the term 'filing date' means the date on which notice of such direct payment procedure was published under section 10(b)."

# Customer Protection

Promptly after appointment, the trustee publishes notice of the proceeding's commencement in one or more newspapers of general circulation. A copy is also mailed to all recorded customers of the debtor with open accounts within the preceding 12 months.

## "Customer" Defined

SIPA's Section 16(2) defines "customers" as persons with claims on account of securities received, acquired or held by the debtor in the ordinary course of its broker-dealer business from or for securities accounts of such persons (1) for safekeeping, (2) with a view to sale, (3) to cover consummated sales, (4) pursuant to purchases, (5) as collateral security, or (6) for purposes of effecting transfer.

The term "customer" also includes persons with claims against the debtor arising from sales or conversions of such securities, and persons who have deposited cash with the debtor for the purpose of purchasing securities. The term does not include, however, persons to the extent that they have claims for property which by contract, agreement, or understanding, or by operation of law, is a part of the capital of the debtor or is subordinated to the claims of the debtor's creditors. Nor does it include any person to the extent that that person's claim arises from transactions with a SIPC member's foreign subsidiary.<sup>32</sup>

A customer is required to file a written statement of claim. A claim form accompanies each notice mailed to customers and claims must be filed within six months after the publication of notice, with a few exceptions.<sup>33</sup>

## Protected Property

SIPA's protections apply to most types of securities, such as notes, stocks, bonds, debentures, and certificates of deposit. No protection, however, is provided for unregistered investment contracts, or for any interest in a commodity contract, or commodity option.

Shares of money market mutual funds, although often viewed as cash, are in fact securities. When held by a SIPC member in a

<sup>32</sup>Sections 16(3) and 3(a)(2)(A)(i).

<sup>33</sup>Section 8(a)(3).

customer's securities account, they are protected as any other covered security. SIPC protection, however, does not cover the decline or loss in value of these or any other securities.

Cash balances are protected under SIPA if the money was deposited or left in a securities account for the purpose of purchasing securities. This is true whether or not the broker pays interest on the cash balances. Of course, cash balances maintained solely for the purpose of earning interest are not protected.

SIPC presumes that cash balances are left in securities accounts for the purpose of purchasing securities. It would require substantial evidence to the contrary to overcome this presumption. Standing alone, the fact that a cash balance was earning interest and was not used to purchase securities for a considerable period of time, say several months, would not be sufficient to overcome the presumption.

## Transfer of Customer Accounts

SIPA authorizes the trustee, with SIPC's approval, to transfer some or all customer accounts to another SIPC member if a transfer will facilitate prompt satisfaction of customer claims and liquidation of the debtor's business. A transfer's feasibility depends upon several factors. These include the condition of the debtor's books and records, and availability of a SIPC member interested in assuming the debtor's customer accounts, capable of handling the transfer and effectively servicing the new accounts.

Minimizing disruption in customer access to their cash and securities is the major purpose of the transfer. A customer whose account has been transferred may deal with the receiving SIPC member or may transfer the account to another broker-dealer.

## Satisfaction of Customer Claims

When a transfer is not feasible, customer claims are satisfied by the trustee in the following manner:

1. "Customer name securities" are distributed first. "Customer name securities" are those

### Location of Customer Protection Proceedings January 1971 - April 1992



Guam - 1

Total: 235

64

securities on hand and registered in a customer's name or were on the filing date in the process of being transferred to the customer's name pursuant to the debtor's instructions. There is no limit on the value of such property which will be returned. Not included, however, are securities on hand which are registered in customer name and in negotiable form. Those securities are considered part of "customer property."

2. Next, the customer's "net equity" is computed for those whose claims were not completely satisfied by the distribution of "customer name securities." "Net equity" is simply the filing date value of securities and cash the debtor owes the customer less any amount the customer owes the debtor.

If a customer has a debit balance, he may, with the trustee's approval and within a time period determined by the trustee, pay the debit balance in order to have a claim for the securities in the account.

Net equity claims are satisfied, to the extent possible, by allocating "customer property" to claimants. "Customer property" means cash and securities (except "customer name securities" delivered to the customer) at any time received, acquired, or held by or for the account of a debtor from or for the securities accounts of a customer. This includes the proceeds of any such property transferred by the debtor, including property unlawfully converted.

Also included in "customer property" are securities options. SIPC has adopted Series 400 Rules, "Satisfaction of Customer Claims For Standardized Options," to establish a uniform procedure for the liquidation and valuation of Standardized Options positions, that is, options traded on a national or foreign securities exchange or on an automated quotation system of a registered securities association. Pursuant to the rule, each customer's options positions will be closed and his account credited or debited, as appropriate, with the value of the options positions on the filing date.

If securities are insufficient to satisfy claims from "customer property," the trustee is obliged to purchase the missing shares if a fair and orderly market exists. If that cannot be done, the trustee allocates available securities pro rata and makes up the shortage by paying customers cash in lieu thereof. The amount paid is based on the value of the securities on the filing date.

One of the questions that regularly arises is whether a customer has a claim for cash or securities. SIPC has adopted Series 500 Rules, "Rules Relating to Satisfaction of 'Claim for Cash' or a 'Claim for Securities'" to establish a uniform procedure for the satisfaction of claims for cash and claims for securities and provide an objective standard for determining each claimant's legitimate expectations. For example, a customer has a "claim for cash," notwithstanding the fact that the customer has ordered the purchase of securities, where the debtor has neither executed the transaction nor sent a confirmation of the purchase. Conversely, a customer has a "claim for securities," notwithstanding the fact the customer has ordered the sale of securities, where the debtor has neither executed the transaction nor sent a confirmation of the sale.

3. If the customer's remaining net equity reflects a long securities position and/or a credit balance, the trustee is obliged to satisfy the claim from SIPC advances up to a maximum of \$500,000 with the following limitation: on claims for cash (as distinct from claims for securities) not more than \$100,000 may be paid from SIPC advances.

Once customer name securities have been returned, customer property distributed pro rata, and SIPC advances provided, up to the limits, any remaining claims are against the debtor's general estate.

In lieu of or as part of the above procedures, the trustee may with SIPC approval sell or otherwise transfer all or any part of a customer's account to another SIPC member as described on page 11. In that connection, the trustee may indemnify the receiving member against shortages of cash or securities in accounts being sold or transferred. SIPC funds may be made available to guarantee or secure the indemnification.<sup>34</sup>

A liquidation's administration cost, that is, fees of the trustee, counsel, accountants, salaries of trustee's employees, and other day-to-day expenses are borne by the debtor's estate to the extent possible. If estate assets are insufficient to pay administration expenses, SIPC makes advances for this purpose.

<sup>34</sup>Section 8(f) requires SIPC to determine that the probable cost of the indemnification is not greater than the cost to SIPC of satisfying claims in the usual fashion.

### Direct Payment Procedure

In certain circumstances SIPC may employ the "Direct Payment Procedure" (DPP). This procedure, added by the 1978 Amendments, addresses criticism that the original Act was too rigid in requiring all liquidations to be handled the same. Prior to the 1978 Amendments, in some very small cases, a court-supervised liquidation incurred a high cost per claim satisfied and paying claims directly would have reduced costs considerably.

Using the standards cited on page 8, if SIPC determines the DPP to be appropriate, notice is published and customers sent notices and claim forms. The publication date is considered the DPP's commencement date and also the filing date for determining securities positions and values.

Upon receipt of claims and appropriate documentation, SIPC satisfies claims much the same as in a court-ordered liquidation. Use of the DPP does not preclude an aggrieved customer from seeking adjudication of SIPC's claim determination, providing action is taken within six months of SIPC's mailing the determination to the customer.

If, after the DPP's initiation, SIPC determines the procedure is inappropriate, it may terminate the DPP and seek appointment of a trustee to carry out a court-ordered liquidation. Whatever claims were wholly or partially satisfied, and whatever claims were recognized as valid under the DPP, would be recognized as such in the liquidation proceeding.

### Advances To Satisfy Customer Claims

Section 9 deals with SIPC advances to trustees to satisfy customers' claims and pay administration expenses. To both satisfy and accelerate payment of the net equities of customers of the debtor, SIPC is to advance to the trustee monies to satisfy claims in full of each customer up to SIPA's limits of protection.

A customer who holds accounts with the debtor in *bona fide* separate capacities is considered a different customer in each capacity. SIPC has adopted Series 100 Rules, or "Rules Identifying Accounts of Separate Customers' of SIPC Members," to further define such separate capacities.

No advance may be made by SIPC to the trustee to satisfy any claim of a customer who

is a general partner, officer, or director of the debtor, a beneficial owner of five per cent or more of any class of equity security of the debtor (other than a nonconvertible stock having fixed preferential dividend and liquidation rights), a limited partner with a participation of five per cent or more in the debtor's net assets or net profits, or a person who, directly or indirectly and through agreement or otherwise, exercised or had the power to exercise a controlling influence over the debtor's management or policies. Nor may SIPC advance funds to satisfy claims of any broker or dealer or bank unless those claims arise from transactions for customers of that broker, dealer or bank, in which event, each such customer is deemed a separate customer of the debtor.

### Advances for Administration

SIPC may advance money to the trustee to hire and pay personnel for the liquidation proceeding, pay other administration expenses, and, as noted below, complete open contractual commitments. Money may also be advanced to pay or guarantee indebtedness of the debtor, guarantee or secure the indemnity of a broker-dealer to which customer accounts are transferred or sold, and purchase securities in the open market to satisfy customer claims.

### *SIPC's Subrogation and Recoupment Rights*

To the extent that monies are advanced to the trustee to satisfy customer claims, SIPC is subrogated to those claims; however, SIPC may not assert its subrogee claim against customer property until the pro rata share of customer property has been allocated to all net equity claimants.

In customer property allocation, however, SIPC has priority for repayment of any advances, made to pay or guarantee loans for recovery of securities pledged by the debtor for those loans. In this respect, SIPC is entitled to receive repayment only to the extent that the securities recovered are allocable to customer property rather than to the debtor's estate.<sup>35</sup>

<sup>35</sup>Sections 8(c)(1)(A) and 6(d).

Finally, priorities of distribution from the general estate are as provided by the Bankruptcy Code.

#### *Open Contractual Commitments*

Under certain conditions, the trustee may complete open contractual commitments made between the debtor and another broker-dealer in the ordinary course of the debtor's business and which were outstanding on the filing date. Because of the subject's complexity, SIPA grants SIPC authority to adopt rules concerning the close-out of such commitments.<sup>36</sup>

If in the close-out of contracts the contra broker-dealer derives a net profit, the broker-dealer must pay it to the trustee. If the broker-dealer realizes a net loss, he may enter a claim against the debtor for the loss. To the extent that the broker-dealer's loss arises from contracts in which he was acting for a customer, he is entitled to receive SIPC advances up to

\$40,000 per customer to cover the loss. If no customer is involved, the broker-dealer's claim is against the general estate as an unsecured creditor.

#### *Assistance in Investigations*

SIPC regularly forwards to the SEC, the National Association of Securities Dealers, and the various exchanges the names of principals and others associated with members placed in liquidation. SIPC and its trustees also cooperate with appropriate law enforcement authorities by forwarding other information.

A number of individuals connected with SIPC members liquidated under SIPA were subjected to administrative and/or criminal actions. Some have been permanently barred from the securities industry, some temporarily suspended, and others convicted and sentenced on criminal charges.<sup>37</sup>

<sup>36</sup>Under the original Act, SIPC did not have authority to adopt rules with respect to close-outs. The Commission, however, had such power. Effective July 25, 1973, the Commission adopted Rule S6d-1 which established detailed procedures for the completion of open contractual commitments. Generally, the rule permitted the completion of fails to receive and fails to deliver between the debtor and another broker-dealer which were made in the ordinary course of the debtor's business and which were outstanding on the filing date. Such open contractual commitments must have arisen from a "current" transaction, as defined in the rule, in which the other broker was acting as agent for a customer (or in which the other dealer was acting for a customer in certain defined principal transactions), and must have been promptly brought-in, sold-out, or closed by delivery of funds and securities in accordance with the provisions of the rule.

The 1978 Amendments, in transferring the rulemaking power to SIPC, specified that Rule S6d-1 was to remain in effect until SIPC adopted its own rules in this regard. In 1979, SIPC adopted "Series 300 Rules" pertaining to closeouts which are virtually the same as the SEC Rule S6d-1.

<sup>37</sup>Section 14(b). "Engaging in Business After Appointment of Trustee or Initiation of Direct Payment Procedure.—It shall be unlawful for any broker or dealer for whom a trustee has been appointed pursuant to this Act or for whom a direct payment procedure has been initiated to engage thereafter in business as a broker or dealer, unless the Commission otherwise determines in the public interest. The Commission may by order bar or suspend for any period, any officer, director, general partner, owner of 10 per centum or more of the voting securities, or controlling person of any broker or dealer for whom a trustee has been appointed pursuant to this Act or for whom a direct payment procedure has been initiated from being or becoming associated with a broker or dealer, if after appropriate notice and opportunity for hearing, the Commission shall determine such bar or suspension to be in the public interest."

## Investor Protection in Perspective

This booklet provides an overview of SIPC's operations and their coordination with the securities industry's operational and regulatory fabric. SIPC's organization and procedures address the primary objective set by Congress and the securities industry at the time of SIPC's inception: to provide greater protection for customers of registered broker-dealers and members of national securities exchanges.

The related objective of increasing investor confidence in securities markets was given further consideration by Congress prior to passage of the Securities Investor Protection Act Amendments of 1978. Participants in the Congressional hearings recognized that membership in SIPC can be an "influential factor in an investor's decision to do business with a particular broker-dealer" and that investor confidence in securities markets can be enhanced by "bringing about additional public awareness of SIPC."<sup>38</sup>

### Member Identification

Congress concluded that public acknowledgement of a broker-dealer's SIPC membership was one effective means of increasing public awareness of SIPC. Section 15(d) of SIPA, as amended, therefore, grants SIPC authority to prescribe by bylaw requirements it deems necessary for a member to provide public notice of its SIPC membership.

SIPC's Board of Directors promulgated Article 11, Section 4, of the SIPC Bylaws ("Advertising Bylaw") requiring members to identify their SIPC membership in offices and in pro-

motional material. Specifically, the Advertising Bylaw, as amended through January 21, 1986, requires each member to display in a prominent place the official SIPC symbol in its principal place of business and each branch office. The official symbol is reproduced below.

Each member must also identify its SIPC membership in promotional material used in or on any newspaper, magazine, radio, television, telephone recording, motion picture, slide presentation, or sign or billboard, except where such inclusion might be misleading.

### Improved Investor Protection

In conclusion, investor protection has improved dramatically since 1970 as the self-regulatory apparatus has been refined, member broker-dealer operations modernized, and more stringent requirements for entry into the industry and higher minimum capital requirements instituted.

The 1978 Amendments improved investor protection by providing more flexible and effective methods of conducting customer protection proceedings, while increasing the amount SIPC could advance for each customer's claim. In 1980, the limits of SIPC advances were further increased to the current maximum of \$500,000 with a limitation of \$100,000 for claims for cash.

Finally, SIPA is a complex statute. Definitive answers to many questions concerning SIPA's application to various persons or situations will depend upon future interpretations and administrative and court decisions.



<sup>38</sup>"Securities Investor Protection Act Amendments of 1977" (sic) Report No. 95-746. Report to the Committee on

Interstate and Foreign Commerce of the House of Representatives. Section by Section Summary, p. 33.

**Board of Directors**

James G. Stearns

*Chairman*

Jesse D. Winzenried

*Vice Chairman*

Thomas J. Healey

George H. Pfau, Jr.

Jerome H. Powell

Michael J. Prell

Frank G. Zarb

**HOW SIPC  
PROTECTS YOU**

**Questions and Answers About SIPC**

**TEXT OF THIS BROCHURE ISSUED BY SIPC  
AND ONLY SIPC MAY MAKE CHANGES**

© Securities Investor Protection Corporation 1992

Securities Investor Protection Corporation  
805 Fifteenth Street, N.W.  
Suite 800  
Washington, D.C. 20005-2207  
(202) 371-8300

---

# Foreword

---

The Securities Investor Protection Corporation (SIPC) protects customers of registered securities broker-dealers, thereby promoting confidence in United States securities markets. Though created by the Securities Investor Protection Act of 1970 (15 U.S.C. §78aaa et seq., as amended), SIPC is neither a government agency nor a regulatory authority. It is a nonprofit, membership corporation, funded by its member securities broker-dealers.

This text answers the most frequently asked questions about how claims are satisfied when securities customers of a member need SIPC protection. Of course, SIPC does not protect against losses from the rise or fall in market value of your investment. It does, however, provide important protections against certain losses if a SIPC member fails financially and is unable to meet obligations to its securities customers.

The Securities Investor Protection Act is a complex and technical statute. While this brochure provides a basic explanation, it does not purport to explain the statute with respect to any particular fact pattern. Answers to questions involving particular facts depend upon interpretations, administrative decisions, and court actions.

**NO PERSON MAY, BY ANY REPRESENTATION, INTERPRETATION, OR OTHERWISE, AFFECT THE EXTENT OF THE COVERAGE PROVIDED CUSTOMERS' ACCOUNTS BY THE ACT OR THE RULES ADOPTED THEREUNDER.**

April, 1992  
Fifth Edition

---

# Contents

---

	<i>Page</i>
<b>Basic Protection</b>	
SIPC Protection	4
"Customer" Defined	5
Property Protected	5
Protected "Securities"	6
Money Market Funds	6
\$100,000 Cash Limitation	6
Accounts at More Than One Broker	7
Several Accounts at One Broker	7
SIPC Fund Protects Customers	8
Dealing With a SIPC Member	9
<b>Customer Protection Proceedings</b>	
Notice to Customers	10
Submitting Claim Forms	10
Return of Customer Securities	10
Securities Valued	11
Return of Customer Property	11
Stock Option Protection	11
Determining Customer Claims	12
Customer Indebtedness	12
Customers Ineligible for Protection	12
<b>Membership and Financing</b>	
Member Broker-Dealers	13
SIPC's Governance	14
Source of Funds	14
Emergency Financing	14
Examination of Membership	15

---

# Basic Protection

---

## 1. What is SIPC's basic protection?

SIPC protects securities customers of member broker-dealers. If a member fails financially SIPC may ask a federal court to appoint a trustee to liquidate the firm and protect its customers, or, in limited situations involving smaller firms, SIPC may protect the customers directly. In both cases, protection of securities customers is similar.

The trustee and SIPC may arrange to have some or all customer accounts transferred to another SIPC member broker-dealer. Customers whose accounts are transferred are notified promptly and permitted to deal with the new firm or subsequently transfer their accounts to firms of their own choosing. Accounts so transferred are subject to the limitations of protection discussed below. This procedure minimizes disruption in customers' trading activities. In many cases (for example, where failed firms' records are inaccurate), account transfers are not feasible. SIPC then protects customer accounts in the following manner:

Customers of a failed firm receive all securities registered in their names or in the process of being so registered and which are not by endorsement or otherwise in negotiable form.

Customers receive, on a pro rata basis, all remaining customer cash and securities held by the firm.

After the above distribution, SIPC's funds are available to satisfy the remaining claims of each customer up to a maximum of \$500,000, including up to \$100,000 on claims for cash (as distinct from claims for securities). When a customer has sold a security, any claim with respect to that transaction would be subject to the \$100,000 limit of protection for cash.

Any remaining assets after payment of liquidation expenses may be available to satisfy any remaining portion of customers' claims on a pro rata basis with other creditors.

---

## 2. Who is a "customer" protected under the Act?

---

"Customers" are persons with claims for securities received, acquired or held by the firm from or for the securities accounts of such persons for safekeeping, with a view to sale, to cover consummated sales, pursuant to purchases, as collateral security, or for purposes of effecting a transfer. Persons who have cash on deposit with a firm for the purpose of purchasing securities or as a result of sales thereof are also considered "customers."

Cash on deposit with a SIPC member for the purpose of earning interest or for any purpose other than purchasing securities is not protected under the Act (see question 3).

A person is not considered a "customer" under the Act to the extent that his claim (a) is for cash or securities which, by contract, agreement, or understanding, or by operation of law, is part of the capital of the firm or is subordinated to the claims of creditors of the firm, or (b) arises out of transactions with a foreign subsidiary of the firm (see question 19 for a discussion of customers who are ineligible to receive money from SIPC).

---

## 3. What property does SIPC protect?

---

Customers' cash and securities: Most types of securities, such as notes, stocks, bonds and certificates of deposit, are covered. No protection, however, is provided for investment contracts which are not registered as securities with the Securities and Exchange Commission under the Securities Act of 1933 or for any interest in gold, silver or other commodity, or commodity contract, or commodity option. It is important to remember, however, that SIPC protection does not cover decline in the market value of securities.

Cash balances are protected under the Securities Investor Protection Act if the money was deposited or left in a securities account for the purpose of purchasing securities. This is true whether or not the broker pays interest on the cash balances. Cash balances maintained solely

for the purpose of earning interest are not protected.

SIPC presumes that cash balances are left in securities accounts for the purpose of purchasing securities. It would require substantial evidence to the contrary to overcome this presumption. Standing alone, the fact that a cash balance was earning interest and was not used to purchase securities for a considerable period of time, say several months, would not be sufficient to overcome the presumption.

---

#### **4. What are protected "securities?"**

---

In addition to notes, stocks, bonds, debentures and certificates of deposit, the term "security" includes investment contracts and certificates of participation or interest in any profit-sharing agreement or in any oil, gas, or mineral royalty or lease if such contracts or interests are registered as securities with the Securities and Exchange Commission under the Securities Act of 1933. Warrants or rights to purchase, sell or subscribe to the securities mentioned above and any other instrument commonly referred to as a security are also protected under the Act.

---

#### **5. Does SIPC protect money market funds?**

---

Shares of money market funds, although often thought of by investors as cash, are in fact securities when such funds are organized as mutual funds. When held by a SIPC member in a customer's securities account, such fund shares are protected as any other covered security.

---

#### **6. Why is cash protection limited to \$100,000?**

---

Two Federal Government agencies have similar limitations on cash claims: the Federal Deposit Insurance Corporation established by

Congress in 1933 and the National Credit Union Administrator's share insurance program authorized in October 1970. Both limit cash protection to \$100,000.

---

#### **7. May a customer have protected accounts with more than one SIPC member?**

---

Yes. Customers' securities accounts with each SIPC member are protected without regard to accounts with other SIPC members.

---

#### **8. May a customer have more than one protected account with the same SIPC member?**

---

Yes, where a customer holds accounts with the same SIPC member in separate capacities. For example, if a person deals with the member in the person's own capacity and also maintains accounts as a trustee for another person under certain trust arrangements, the person would be deemed a different customer in each capacity. A customer having several different accounts must be acting in a good faith separate capacity with respect to each.

An investor might, for example, have one account in his or her name and maintain a joint account with his or her spouse, providing each possesses authority to act with respect to the entire account.

All such accounts, however, must meet the requirements of SIPC rules identifying accounts of "separate" customers of SIPC members. Copies of these rules may be obtained by writing to SIPC and requesting the "Series 100 Rules."

A person who in a single capacity has several different accounts with the same firm, e.g., cash and margin, would be considered a single customer for purposes of applying the \$500,000/\$100,000 limits.

72

## 9. How does SIPC's Fund protect customers?

The examples below apply to claims remaining after the return to customers of securities registered in their names and after the pro rata distribution of "Customer Property" held by the firm (see question 1).

- A remaining claim is for \$400,000 in securities. The claim would be satisfied in full.
- A customer has a claim for \$400,000 in securities in an individual account and for \$500,000 in securities in a joint account with his or her spouse, as to which each has full authority. The spouse also has an individual account in which there is a claim for \$400,000 in securities. All three claims would be fully covered.
- A customer has a claim for \$730,000 in securities in a margin account, but he owes the broker \$230,000 on those securities. The customer's "net equity" would be \$500,000 and would be fully covered. With the trustee's approval, the customer may pay the \$230,000 and receive the \$730,000 in securities (see question 18).
- A remaining claim is for \$420,000 in securities and \$100,000 in cash. All but \$20,000 would be covered.
- A remaining claim is for \$30,000 in securities and \$110,000 in cash. The claim would be covered to the amount of \$130,000 (\$30,000 for securities and \$100,000 for cash).
- A customer has a claim for \$550,000 in securities and \$120,000 in cash. The claim would be covered to the amount of \$500,000 (the maximum).

In the last three examples, any portion of the claim remaining may be satisfied in part from assets of the failed firm if any are available for distribution to creditors.

## 10. How can I be sure I am dealing with a SIPC member?

SIPC members display this sign:



If you have a question as to whether a firm is a member of SIPC, you may call or write to our Membership Department at the telephone number or address on the title page of this brochure.

Some SIPC members have affiliated or related companies or persons who conduct financial or investment businesses but who are *not* members of SIPC. Some of these affiliates have names which are similar to the name of the SIPC member, or which operate from the same offices or with the same employees. Be sure you receive written confirmation of each securities transaction in your securities account with the SIPC member, and *that each confirmation statement and each statement of account is issued by the SIPC member and not by a non-SIPC member affiliate*. Deposits for credit for your securities account, by check or otherwise, should not be made payable to your account executive, registered representative, or to any other individual, but generally only to your SIPC member broker-dealer or, if your account is carried at another SIPC member who provides clearing services for your SIPC member broker-dealer, then to that other SIPC member. If your check or deposit is payable to other than a SIPC member broker-dealer (such as to the issuer of the securities you are purchasing or to a bank escrow agent), you should take steps to insure that your funds are properly applied.

# Customer Protection Proceedings

## 11. How do customers learn that their broker has been placed in liquidation?

Notice will be published in one or more newspapers of general circulation and a copy together with a claim form mailed to each customer's address as it appears from the broker's books and records.

## 12. To whom does a customer submit a claim form?

Directly to the trustee; if no trustee has been appointed, directly to SIPC. The notice and claim form (referred to above) will give instructions.

It is important that customers submit their completed claim forms promptly within the time limits set forth in the notice and in accordance with the instructions to the claim form. Failure to do so may result in the loss of all or a portion of a customer's claim for funds and securities.

## 13. Will a customer get back all of the securities in the account?

Usually, yes; but sometimes no. Here's why:

For various reasons, a failed firm may not have all customer securities on hand. The trustee attempts to purchase such missing securities in the market, providing a fair and orderly market for the securities can be found.

When missing securities cannot be replaced by market purchases, the customer receives cash based on the market value of the securities as of the value date (see question 14).

## 14. How is a customer's claim for securities valued?

Claims are valued as of a date prescribed by the Act ("value date"), generally the day customer protection proceedings commence.

To the extent possible (as indicated above), claims for securities are satisfied by delivering securities to customers. The amount of cash paid instead of securities reflects their worth on the value date and may, of course, differ from the securities' value on the date payment is made.

## 15. How quickly can a customer expect to receive property in the account?

This will vary from proceeding to proceeding. As a general rule, most customers can expect to receive their property in one to three months. When the records of the firm are accurate, deliveries of some securities and cash to customers may begin shortly after the trustee receives the completed claim forms from customers, or even earlier if the trustee can transfer customer accounts to another broker-dealer. On the other hand, there may be delays of several months where the firm's records are not accurate, or where it appears that the firm or its principals were involved in fraudulent activities. Some delays also may be caused by the need to send stock certificates to transfer agents with specific instructions to issue smaller denominations and issue certificates in other names. This can be a time-consuming operation.

## 16. How are stock options protected?

All exchange-traded securities option positions will be closed and customers who have claims for such positions will, within the statutory limits, be paid the market value of those positions on the value date (see question 14). The trustee, in his sole discretion, may choose not to close some covered short positions when the customer's broker has caused the cover to be depos-

ited with either its correspondent broker or the Options Clearing Corporation. The fact that the customer has given his broker the underlying securities does not guarantee the position is covered for purposes of a SIPC liquidation proceeding.

**17. How is the amount of a customer's claim determined?**

The amount of the customer's claim, excluding any securities registered in his name and returned to him, is called his "net equity." The net equity of a customer's account is determined by adding the total value of cash and securities the firm owes the customer and subtracting the total value of cash and securities the customer owes the firm.

**18. Must the customer pay what he owed the firm to the trustee?**

Usually no, because indebtedness is taken into account in computing a customer's net equity and the customer will receive a pro rata share of the securities in the account valued as of the value date. However, with the trustee's approval and within a time period determined by the trustee but not exceeding 60 days from publication of the notice described in question 11, the customer may pay the debit balance and receive all of the securities in the account subject to the limitations described in question 1.

When the customer owes the firm more than the firm owes the customer, the customer must pay the difference to the trustee.

**19. Which customers are ineligible for protection from SIPC funds?**

SIPC's funds may not be used to pay claims of any customer who also is: (1) a general partner, officer, or director of the firm; (2) the beneficial owner of five percent or more of any class of equity security of the firm (other than certain nonconvertible preferred stocks); (3) a limited partner with a participation of five percent or

12

more in the net assets or net profits of the firm; (4) someone with the power to exercise a controlling influence over the management or policies of the firm; or (5) a broker or dealer or bank acting for itself rather than for its own customer or customers.

## Membership and Financing

**20. Who are members of SIPC?**

Broker-dealers registered with the Securities and Exchange Commission (other than banks registered as municipal securities dealers) whose principal business is conducted within the United States, its territories or possessions are automatically members of SIPC with two exceptions:

- Broker-dealers whose business as a broker-dealer is exclusively (1) the distribution of shares of mutual funds, (2) the sale of variable annuities, (3) the business of insurance, or (4) the furnishing of investment advice to investment companies or insurance company separate accounts.
- Broker-dealers whose securities business is limited to United States Government securities and who are registered with the Securities and Exchange Commission under a provision of law which does not confer SIPC membership. Investors interested in whether a particular government securities dealer is a member of SIPC should make appropriate inquiries.

A SIPC member displays this sign:



See also question 10.

---

### **Who runs SIPC?**

---

Board of Directors, which consists of seven members. Five are appointed by the President of the United States (subject to Senate confirmation), of whom two are representatives of the public and three, the securities industry. In the public members, the President appoints the Chairman and Vice Chairman. In the industry member each is designated by the Secretary of the Treasury and the Federal Reserve Board from among their respective employees.

The Securities and Exchange Commission has oversight and regulatory functions with respect to SIPC.

---

### **How does SIPC get its money?**

---

SIPC is required to protect customers' claims which is available from the property of the failed broker-dealer is provided to SIPC from a fund maintained for this purpose. The sources of money for the SIPC are industry assessments collected from SIPC members and interest on investments in United States government securities.

---

### **What emergency financing in the event the SIPC Fund is insufficient?**

---

In an emergency, SIPC may borrow up to \$500 million from the U.S. Treasury through the Securities and Exchange Commission if the Commission determines such a loan is necessary to protect investors and maintain confidence in the securities markets. SIPC must provide a plan which provides as reasonable an assurance of prompt repayment as may be feasible under the circumstances. If the Commission determines industry assessments would not satisfy the loan, it may impose a transaction fee on purchasers of equity securities at a rate of 1/50 of 1% of the purchase price (per \$1,000). This fee would not apply to purchases of less than \$5,000.

---

### **24. Who examines the operational and financial conditions of SIPC members?**

---

The securities exchanges and the National Association of Securities Dealers, Inc. (NASD) are the "examining authorities" for SIPC members. SIPC has no authority to examine or inspect its members.

---

---

**A Bankwide Assessment of Risks Associated With  
Traditional and Non-Traditional Services  
and New Business Opportunities**

**RISK ASSESSMENTS:  
WHOLESALE WIRE PAYMENTS SYSTEMS**

by Robert Listfield

*Sue  
FYB  
Jou*

 **AMERICAN  
BANKERS  
ASSOCIATION**  
1120 Connecticut Avenue, N.W.  
Washington, D.C. 20036

---

---

# Table of Contents

	Page
Foreword .....	vii
Preface .....	ix
Executive Summary .....	xi
<b>CHAPTER 1</b>	
<b>Overview .....</b>	<b>1</b>
Introduction .....	1
The Wholesale EFT Process and Its Risks .....	2
Potential Liabilities .....	4
The Four Major Wholesale Electronic Payments Systems .....	5
<b>CHAPTER 2</b>	
<b>Risks in Wholesale Payments and Methods of Reducing     Those Risks .....</b>	<b>9</b>
Operating Risk .....	9
Fraud Risk .....	11
Credit Risk .....	14
FedWire .....	15
CHIPS .....	16
CashWire .....	16
Techniques for Minimizing Credit Risk .....	16
Risk of Service Disruption .....	17
<b>CHAPTER 3</b>	
<b>Risk Control and Risk Transfer .....</b>	<b>19</b>
Risk Control .....	19
Risk Transfer .....	19
Insurance .....	19
Legal Agreements .....	20
Charges to the Customer .....	21

Future Risk Control ..... 21  
Federal Reserve's Attempts to Limit Risk ..... 22

**CHAPTER 4**

**Summary and Conclusions ..... 23**

**APPENDIX 1**

**Sample Checklist of Major Vulnerabilities, Control  
Procedures, and Organizational Responsibilities ..... 25**

**APPENDIX 2**

**Rules of the Nationwide Task Force on Uniform  
Compensation ..... 29**

19

---

# Foreword

Dear Colleague:

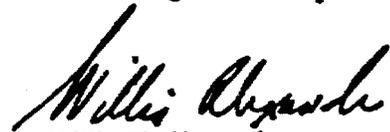
Dealing with risk is a part of the life of every business, but this is especially true for banks. The very nature of banking creates unique types and levels of risk. In addition, the growing sophistication of operations linked to the banking industry's diversification into related financial services exposes banks to types of risk not experienced in the past.

Your fellow bankers who serve on ABA's Banking Professions Council recognized the need for a management tool which will help the industry to identify, analyze, and control the risks associated with a changing banking environment. As such, the Council commissioned a major ongoing bank-wide assessment of risk associated with tradi-

tional and non-traditional services and new business opportunities.

The result of these assessments will be reports such as this one distributed as an ongoing membership service which will help you and your bank to better assess and manage your risks, both existing and emerging.

Reliance upon this risk management process, as a legitimate management tool for protecting a bank's assets, may well determine the success of any banking institution, its profitability, and the continuation of public confidence, which is the cornerstone of banking.



Willis W. Alexander  
Executive Vice President  
American Bankers Association

---

# Preface

This report explores the major elements of risk in wholesale electronic funds transfer systems (FedWire, Clearing House Interbank Payments System [CHIPS], Cash-Wire, and Corporate-to-Corporate ACH) and outlines steps that should be taken to reduce the prospect of a large financial loss to an organization. Because of the large sums of money transferred daily through using wholesale electronic funds transfer systems (EFTS), the potential loss exposure is great. Unfortunately, however, no data are available on the frequency or magnitude of wholesale EFT losses, so that the absolute potential for loss cannot be quantified.

Chapter 1 provides background material. Chapter 2 describes the four major types of wholesale EFT risk (operating error, fraud, credit exposure, and disruption of service), identifying banks' vulnerability to these risks and outlining steps to minimize them. Chapter 3 describes methods of transfer-

ring them, either through insurance or legal agreements. Chapter 4 is a summary and conclusion. Appendix 1 summarizes the major control steps that can be taken and suggests possible assignments or responsibility for ensuring their completion, while Appendix 2 presents the rules formulated by the Nationwide Task Force on Uniform Compensation.

This report provides suggestions to banks with both small and large volumes of wholesale electronic funds transfers. However, because of the variety of operating systems and procedures employed in such transfers, it is not possible to quantify all the risk exposure points in every operation or detail every step that should be taken to minimize those risks. Rather, the report alerts readers to the most common vulnerabilities and controls and provides guidance and a conceptual framework for adapting these concepts to each organization.

---

# Executive Summary

The management of risk is certainly not a new subject for the banking industry. Indeed, the banking industry by its very nature acquires risk as a result of its normal business. Non-traditional risk, however, is all too often ignored by management until a major crisis, such as Drysdale Securities or Penn Square, focuses attention on the problem. Unfortunately, paying attention after the fact could mean losses of untold millions. Furthermore, because risk management must be an inherent part of systems design, paying attention to risk after the fact could also mean undergoing major systems redevelopment, which is both expensive and time-consuming. Ideally, therefore, the management of risk should be a basic part of the system design in all functional areas—and in particular in the payments system.

The payments system merits special attention because improved technology, high interest rates, and the expansion of national and international commerce have produced a situation in which huge sums of money are being transferred between banks every day. Large money-center banks, and even many smaller banks, may transfer many times their total assets in a given day, and the banking industry as a whole transfers the equivalent of the gross national product of the United States almost every seven days and the equivalent of the national debt in less than every three days. The movement of such large sums of money is bound to create certain elements of risk in a variety of forms.

Corporate electronic funds transfers, in particular, merit a risk control program, not

only because of the high-dollar value of funds transferred (the two principal funds transfer services, FedWire and CHIPS, transfer approximately \$560 billion dollars a day), but also because of the amount of credit exposure that funds transfer participants undertake, the lack of any formalized law governing wholesale EFT, and the degree to which responsibility for corporate EFT risk control cuts across departmental lines.

The large dollar value transferred makes the threat of loss from fraud or operating error quite large for most organizations. It is therefore important for banks to have comprehensive controls to minimize the prospect of tampering or of unauthorized messages being initiated and to provide sufficient control checks to guard against inadvertent operating errors.

The issue of funds transfer credit exposure is one that has only recently been identified as a critical issue by the Federal Reserve and many leaders in corporate EFT activity. Corporate EFT systems occur when funds are transferred out of customer accounts, regardless of the customer, without their authorization collected funds in the customer's account against which to charge. Because account balances can turn over several times in one day, many banks do not always know whether transfers are made against collected funds in their customer's account. Even if the systems existed to enable a bank to monitor account balances on a real time basis, the speed at which transfers are made would not lend itself to the types of deliberate credit-extension decisions that

are normally made in banking. Banks should be aware that credit decisions are being made, either explicitly or implicitly, in the corporate EFT area, and that such credit decisions may require greater scrutiny than they now receive.

The absence of a formalized law covering wholesale EFT means that the major legal framework for corporate EFT must be documented in the legal agreement between banks and their customers. To provide maximum protection, the legal agreement should clearly assign the rights and responsibilities between a bank and its customer and should be reviewed and updated frequently.

A bank should transfer the risk it cannot control. Risk can be transferred through insurance, through legal agreements, and through charges to customers. The bank should accept liability for what is under its

own control and should pass on to customers, liability for what they can control.

Banks, to be sure, can and should institute effective programs to identify and control their risks and should monitor these programs. This study details the problem and suggests a variety of possible ways of coping with it.

Finally, responsibility for risk management rests not with one person or department but with the entire organization. This study should therefore be reviewed, in whole or at least in part, by the following: Chief Operating Officer, Security Officer, Personnel Officer, Funds Transfer Operating Officer, Legal Department, Credit Officer, Corporation and Correspondent Bank Calling Officer/Account Executive, Audit Department, Risk Management Officer, and Data Processing Officer.

83

# CHAPTER ONE

## Overview

### INTRODUCTION

Banks using wholesale electronic funds transfer systems (EFTs) are essentially extending **instant credit** amounting to billions of dollars a day. Since these transactions are not governed by a formalized law or an equivalent system of controls, the risks are great; and as the volume of funds transfers increases, the risks become greater. To guard against the risks and to discover losses early, banks need to institute a system of controls monitored on a regular schedule and flexible enough to respond to whatever changes take place in the kind and degree of risk.

With these considerations in mind, this study will focus on the mechanics of the various types of EFT systems banks use and the types of risks involved, and then present possible controls.

Today, FedWire, CHIPS, CashWire, and ACH corporate-to-corporate payments are the major wholesale EFT systems used by banks; and operating risk, fraud, credit exposure, and disruption of service are the major risks banks face in the electronic world of banking.

**Operating risk**, or any *inadvertent* action that causes a loss of money, goods, or services (or good will) to a bank or its customers, is **caused primarily by human error**. **Fraud**, on the other hand, involves an **intentional action** that causes a loss of money, goods, or services to a bank or its customers. Fraudulent transfer requests, alteration of the terms of a valid request, destruction of records to erase a valid

transfer, and inadvertent alteration, misdirection, or duplication that results in unauthorized recipients' absconding with the funds are the chief kinds of fraud risk.

Credit exposure, essentially a result of funds transfers being generally both instantaneous and irrevocable, leaves a bank in a vulnerable position because a bank cannot guarantee that the funds will be paid. Disruption of services also can be costly and, therefore, contingency backup procedures or facilities are necessary.

For the bank, these risks create the possibility of legal action involving liability for lost earnings, liability for principal, and consequential damages.

**Operating risk to be minimized**, requires a concerted effort of **logging and balancing**; thoroughly **training** operators; using call-back; **entering data twice** or having data be **independently verified**; minimizing the need for manual intervention; allowing ample time between the deadlines to customers and the networks' deadlines; adequately developing and testing software; reconciling accounts without excessive delay; and being **careful** when using **suspense accounts**.

Authentication codes, callback, on-line access, tight security of wire rooms, special security program edits, reconciliation, and data encryption are methods of controlling fraud risk.

By using the same approach to funds transfers that it uses in loan authorizations, a bank can control credit risk. The bank should know whether the loan is collateralized or not. In turn, the wire networks can minimize credit risk among their mem-

bers through on-line accounting systems, bilateral credit arrangements, and credit caps.

To minimize the risk of loss due to disruption of service, a bank can duplicate its facilities, become a member of more than one network, and train its staff to operate in an off-line mode.

Banks that now have a risk control program for corporate electronic funds transfers should continuously review and update their programs because the magnitude and nature of the risks change. One of the principal recent changes associated with corporate EFT is the increase in the number of direct funds transfer participants and the consequent increase in volume.

With the expanded access to FedWire that resulted from the Monetary Control Act of 1980, many more institutions became directly involved in funds transfer activity; and transfer volume continued to grow. Both of these changes increase the risk for each institution.

A second major change connected with corporate EFT is the increased use of on-line connections. Many smaller banks have recently converted their funds transfer system from origination and receipt by telephone (off-line) to origination and receipt by terminal (on-line). And many larger banks have been converting their corporate and correspondent bank customers from off-line to on-line terminal interfaces. Moreover, as customers convert to on-line, they tend to increase the volumes of their funds transfers—changing not only the nature, but also the magnitude, of the risk.

A third major change associated with corporate EFT is that the public's knowledge of computers has increased, which means an increased risk of fraud or manipulation of data.

Banks that already have a control program and banks that are about to create one may, in both cases, find it helpful to draw up a security checklist similar to that in appendix 1. The checklist can provide more detailed control procedures relevant

to the bank's unique operating environment and can assign responsibility for each security step to specific individuals.

One effective way of developing and continuously improving a risk management program is for a bank to compare its own internal operations and its customer interfaces to the control concepts and procedures used by its funds transfer network supplier (FedWire, CHIPS, CashWire). Because of the dollar volumes these operators handle, they have necessarily developed sophisticated control procedures to guard their networks and, for the overall security of the service, would be happy to share control concepts with users.

Banks must recognize that total elimination of risk in funds transfers is, of course, impossible; but the risk can be managed, allowing senior management to assess the trade-off between the prospects for loss and the cost of risk control procedures that minimize the likelihood of large losses.

The purpose of this study, then, is to provide a framework for analyzing risk in wholesale wire payments systems so that payments system managers can better identify risks within their own organizations and develop on-going programs to control such risks. The study addresses the risks inherent only in wholesale, electronic-based payments systems, discussing funds transfers systems (FedWire, CHIPS, and CashWire) and ACH corporate-to-corporate payments. SWIFT, BankWire, and Telex, since they transfer payment instructions rather than funds, are not discussed separately (although many of the control concepts presented can and should be applied to those systems as well).

## THE WHOLESALE EFT PROCESS AND ITS RISKS

Wholesale EFT transfers are generally credit transfers (transfers of funds from the originator to the receiver of the transfer)

made in payment of an immediate, high-dollar obligation or to enable the recipient to make immediate use of the funds. The transfers are generally made through an electronic funds transfer network, such as FedWire, CHIPS, CashWire, or the Automated Clearing House (ACH). Examples of some of the more common types of wholesale EFT payments include—

- the transfer of Fed funds bought from the selling bank to the buying bank;
- the return of bought Fed funds to the selling bank;
- the transfer of correspondent bank balances between banks;
- a corporation's transfer of funds between banks to concentrate corporate balances into one bank for cash management purposes;
- the transfer of funds between corporations to secure a contract or pay an obligation;
- a corporation's or bank's transfer of funds to another bank for investment purposes; and
- an individual's transfer of balances between banks for a large dollar investment (usually real estate) or to close an account because of a relocation.

As the examples show, funds transfers may originate at the request of a correspondent bank, at the request of a corporate or individual customer of the bank, or within the bank itself, and may be destined for another bank or for the bank's customer. Virtually all wholesale EFT transfers (except those for which the originator and recipient accounts are held at the same bank) are sent through a funds transfer network (FedWire, CHIPS, CashWire, ACH) rather than directly between banks. The originator of the funds transfer request must designate the dollar value of the transfer, the receiving bank, and any third-party beneficiary (e.g., the corporation, correspondent bank, or individual that is to

receive the funds), and may also provide any special payment instructions, such as the purpose of the transfer (e.g., return of Fed funds).

The originator of the request may give payment instructions to the originating bank via telephone, paper request, or terminal. The originating bank will verify the authenticity of the transfer (to be discussed in later sections); select the funds transfer network to be used (or, in some cases, will have the originator specify the network); debit the originator's account; and transmit the payment instructions to the network operator. The payment instructions can be transmitted (a) telephonically to the network operator (in the case of FedWire), (b) via terminal or direct computer-to-computer link, or (c) by magnetic tape (in the case of the ACH).

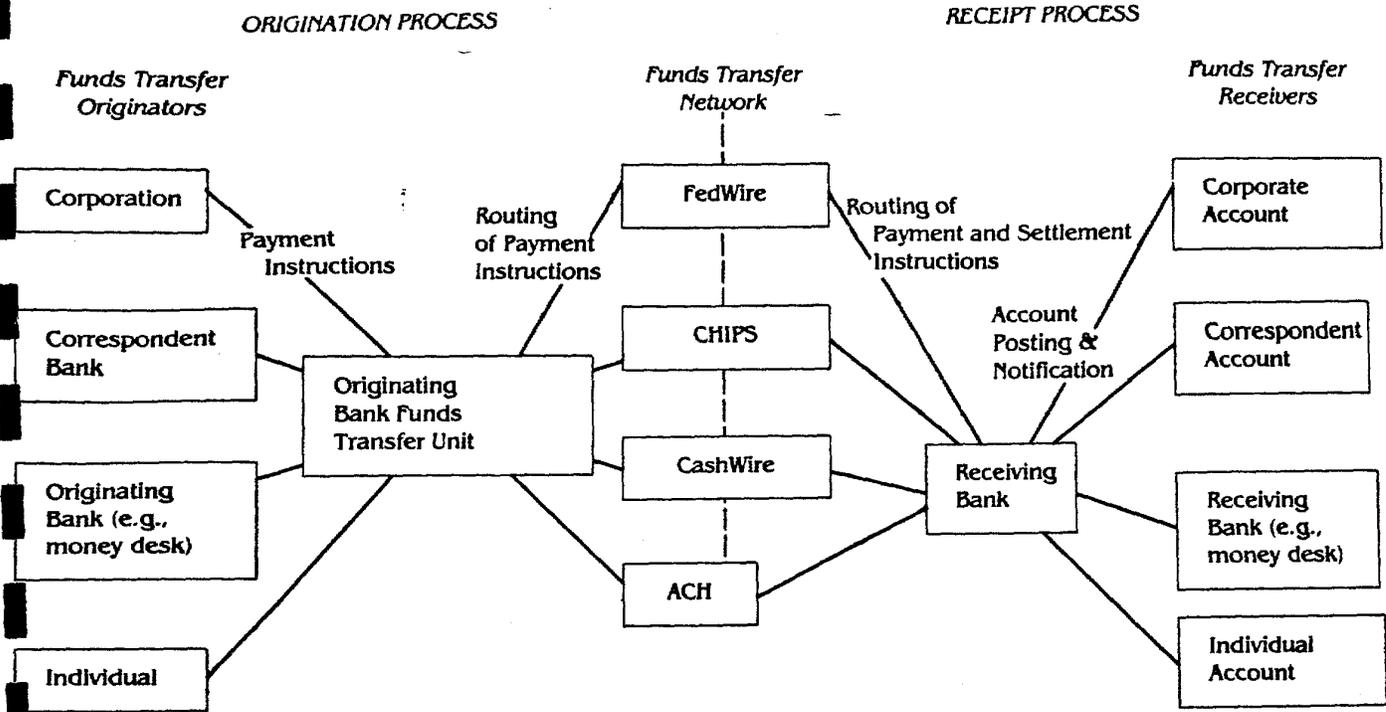
The funds transfer network operator receives the payment instruction from the originating bank, verifies authenticity, makes the necessary settlement entries (debit to the originating bank and credit to the receiving bank), and then routes the transfer to the receiving bank. This transmission, too, can be done (a) telephonically (for FedWire), (b) to a terminal or computer at the receiving bank, or (c) via magnetic tape or paper listing (for the ACH).

The bank receiving the funds will verify the authenticity of the source, update the account of the payment recipient, and notify the recipient of receipt of the funds. This notification is generally done via paper (statement of account balance), telephone, or terminal.

Figure 1 diagrams the entire process.

As is discussed in the next chapter, vulnerabilities exist at each point at which the payment instructions are passed between parties. (And the vulnerabilities, as well as the controls needed to reduce risk, are similar for the three parties involved—the originating bank, the network operator, and the receiving bank—each of whom must receive, verify, route, and settle payment instructions.) These vulnerabilities include the possibility of unauthorized orig-

**Figure 1**  
**Diagram of Wholesale EFT Process**



ination or alteration of data (**fraud**); the inadvertent alteration, omission, or duplication of data (**operating error**); the transfer of funds without the originator's having sufficient balances (**credit risk**); and the **disruption of service**.

## POTENTIAL LIABILITIES

The four risks inherent in wholesale payments systems create the potential for **three types of liabilities**—liability for **lost earnings**, liability for **principal**, and **consequential damages**.

Failing to make timely credit, or inadvertently crediting for the wrong amount, could result in a bank's being liable for the lost earnings on those funds. Although compensation for lost earnings is the lowest cost element of risk in wholesale payments systems, it is by no means trivial. At a 10 percent rate on funds, a delay on a \$10 million transfer is still worth almost

\$3,000 per day in lost earnings to the intended recipient.

If a bank erroneously sends a transfer to a wrong party, or to the right party but for too large an amount, the sending bank may be liable for the value of that transfer if the value cannot be recovered from the receiver. Even if the value can be recovered, recovery may entail a long and costly legal process, and the **bank may not recover its earnings on the funds until they can be recovered and transferred properly**.

Often a corporation will request a transfer of funds to meet some need for a large payment in connection with the signing of a contract or some other business deal. Failure to have such funds available when the deal is scheduled for closing may result in cancellation of the contract. The question of **consequential damages for failure to perform continues to be one of the most ambiguous areas in payments system law**. If a corporation loses a large business deal because of a bank's errors or omissions,

87

the bank may be held accountable not only for the funds that were not transferred, but also for the value to the corporation of the forfeited business venture. Questions of consequential damage will probably be decided by the courts on a case-by-case basis. In one recent case, a \$2.1 million award against a bank was made because a late transfer of \$27 thousand caused the cancellation of a large business deal, although this decision was subsequently reversed by a higher court.

## THE FOUR MAJOR WHOLESALE ELECTRONIC PAYMENTS SYSTEMS

This report treats four major wholesale electronic payments systems—FedWire, CHIPS, CashWire, and ACH Corporate Trade Payments. Each has its own characteristics, which affect the degree of risk to the user, and each has its own method of limiting its internal risk.

### FedWire

FedWire is the Federal Reserve's wire transfer network, and in terms of volume, dollar value, and number of users, it is the largest wholesale EFT network. Its predecessor dates back to 1913, when the Federal Reserve System was established. Over the years, the Fed's wire communications system was improved to provide faster service and to make possible a larger volume of transactions. By 1973 the FedWire system was fully automated, with banks able to originate and receive funds transfers electronically. The current system is now being upgraded to improve network capacity, security, and functionality.

During 1983, FedWire handled about 38 million transactions for an aggregate dollar value of \$85 trillion. Its average dollar value per transaction was about \$2.2 million.

FedWire can be used by any depository institution that has either a reserve account or a clearing account with the Federal Reserve. More than 4,000 of FedWire's participants are connected directly to the Federal Reserve computers, through either a computer-computer interface, a leased-line terminal connection, or a dial-up terminal connection. These institutions are referred to as being on-line. Some 3,000 other institutions, smaller and less active participants, use FedWire by telephone followed by a paper confirmation. These institutions are referred to as off-line users.

Transfers over FedWire are considered to be both immediate and irrevocable, with the Federal Reserve guaranteeing the payment to the receiving financial institution. The settlement day is the day that funds are available for use by the recipient, and finality of payment refers to the day on which the funds can no longer be revoked from the recipient. In the case of FedWire, then, settlement and finality occur as the transfer is made; in the case of CHIPS, settlement (i.e., availability of funds) occurs immediately, but the funds can be revoked on the same evening. With CashWire, settlement is immediate, but finality does not take place until the next morning.

~~Because FedWire transfers are final and guaranteed, there is no settlement risk to either the originator or the receiver of FedWire transfers. That is, if an originating financial institution fails and cannot cover its transfer, the Federal Reserve will cover the loss rather than transfer it to the receiver.~~

### CHIPS

CHIPS, which stands for Clearing House Interbank Payments System, is operated by the New York City Clearing House Association (NYCHA) and is governed by rules and regulations established by the New York Clearing House committee. The CHIPS system was developed in 1970 to handle the dollar settlement of foreign-ordered payments transactions among member and nonmember banks.

In terms of dollars transferred, CHIPS is the second largest wholesale payments system. In 1983 it had a volume of 20 million transfers with a total dollar value of \$60 trillion. The average dollar value per transaction was higher than for FedWire—\$3.0 million per transfer. Currently, CHIPS has 21 settling members, (11 NYCHA members and 10 non-NYCHA members). There are approximately 125 banks that participate and settle through a correspondent relationship with one of the 11 NYCHA members.

Before October 1, 1981, funds transferred through CHIPS were settled on a next-day basis. To eliminate the overnight and overweekend risk within CHIPS, it was decided that CHIPS should process its transactions on a same-day basis. Since October 1, 1981, therefore, CHIPS transactions have been settled at the end of the day, through a settlement arrangement with the New York Fed. But because CHIPS payments, unlike those for FedWire, are not final until the end of the day, ~~participants in CHIPS absorb an intraday risk that at the close of business, the settlement will not be made final.~~

## CashWire

~~CashWire~~ is a new form of same-day settlement service offered by ~~BankWire~~, which is a user-cooperative organization that seven banks created in 1952 as a private communications system. Participation in BankWire is limited to members of the cooperative corporation, and any bank may apply for membership. Currently about 176 members of the corporation use BankWire to deliver funds transfer and administrative messages between banks. Settlement of BankWire funds transfer instructions must be accomplished through correspondent bank relationships.

In September 1982, CashWire was instituted to give participating banks same-day net settlement, and it is currently being used by twenty three banks nationwide.

Over 50 other banks are expected to join in 1984. As of April 1984, CashWire handles

600 transfers per day with the average value per transfer about \$800 thousand.

Credit for ~~CashWire~~ payments is made on a same-day basis, but settlement is not final until 9 A.M. the following day as per a settlement agreement between BankWire (as the settlement agent for the CashWire service) and the Federal Reserve. To effect settlement, BankWire submits to the Federal Reserve, by close of business, the net debit and credit positions for all participating institutions on that day, and the Federal Reserve posts these entries to the participating banks' reserve accounts.

In the event one of the institutions were to fail or have insufficient funds in the reserve account to cover its net debit position, BankWire, as settlement agent, would submit an adjusted settlement statement to the Fed, allocating the net debit of the failed bank to those banks which were net creditors of the failed bank on the day of failure, in proportion to each creditor bank's share of the total of the net credit positions of the creditor banks.

~~To limit the potential loss~~ caused by a failure to settle, ~~CashWire~~ has instituted ~~bilateral credit limits~~ for transfers made between any two parties using the CashWire system. Each bank sets a credit limit for every participant in CashWire with which a bank chooses to exchange CashWires. If a transfer is originated that would bring the net debit position of one bank above its limit with another, CashWire also has ~~that limits the total net debit~~ position of any participant to 50 percent of its ~~cap~~ (the Federal Reserve agreed to perform the net settlement only if CashWire implemented the debit caps).

## ACH Corporate Trade Payments

The Automated Clearing House (ACH) has been used for several years as a paperless replacement for the check, handling pre-authorized debits (such as insurance payments) and credits (such as payroll and dividends). In 1983, the ACH handled roughly 200,000 commercial items, with an average value per transfer of approximately

\$600. Most of the transfers going to the ACH, however, are payments made between a corporation and an individual and thus would not be considered wholesale electronic payments. Currently the only wholesale electronic payment flowing through the ACH is corporate cash concentration debits whose average dollar value is about \$20,000.

The National Automated Clearing House Association (NACHA) has recently begun a pilot program of corporate-to-corporate trade payments whereby corporations can use the ACH to pay other corporations for goods and services. Because the ACH is capable of handling both debit and credit

transactions, corporate-to-corporate transactions may be in the form of either a payment made from a corporation to its supplier or a withdrawal of funds by the supplier from the purchaser of the services.

Because the ACH corporate trade payments program is still in its infancy, it is too early to tell what kind of volume will shift to the ACH or whether the service will be used primarily as a debit service or a credit service. If it becomes primarily a credit payment service, the risks involved will be similar to those of the funds transfer systems, and therefore the precautions for dealing with the risk will be much the same as for the funds transfer system.

## CHAPTER TWO

# Risks in Wholesale Payments and Methods of Reducing Those Risks

The four most typical types of risk in wholesale payments systems are operating risk, fraud risk, credit risk, and risk of service disruption. In this chapter these risks are discussed in terms of—

- the type and magnitude of the risk assumed;
- methods of controlling and reducing the risk;
- ways of maintaining such risk control methods on an ongoing basis; and
- ways of transferring the remaining risk, either through insurance or through charges to the customer.

### OPERATING RISK

Operating risk is risk from any inadvertent act that causes a bank or its customer to lose money, goods, or services—or customer satisfaction. Operating risk occurs because, as with all operations involving some degree of human intervention, errors can happen. These errors can cause a funds transfer to be directed to a wrong party, to be directed to the proper party but for a wrong amount, to be not sent at all, or to be sent twice. Since the frequency of such errors is quite low, there is relatively little payments system case law or custom governing what happens when such operating errors are made. Nevertheless, such errors can happen and may cause a financial loss—which may be large, since the resulting liability can be for principal, interest, or consequential damages. In fact,

because of the potential liability for consequential damages, the magnitude of the risk can be several times higher than the actual dollar value of the transfer.

The major types of operating risk are—

- failure to initiate a transfer;
- initiation of a transfer for the wrong amount or to the wrong beneficiary; and
- initiation of a duplicate transfer.

The principal methods of minimizing the potential for operating error are discussed below.

**Logging/Balancing.** All incoming transfer requests should be logged in—manually for those received off-line, and by automation for those received on-line. Periodically, but at least before the end of each day, incoming transfer requests should be balanced (both by number and dollar value) against outgoing and pending transfers. Any discrepancies should be rectified on a same-day basis, if possible. This procedure will make immediately evident any missing or duplicate transfers or those for an erroneous dollar value.

**Operator Training.** Because manual operations are generally most susceptible to procedural breakdowns, banks should both minimize the necessity for operator intervention and make sure operators are well trained when such intervention is necessary. Besides being well trained in their responsibilities, operators should have written procedures manuals readily available.

**Callback Procedure.** As in the case of fraud prevention, operator callback is a

good way of verifying not only the authenticity of the request but also the accuracy of the data received. Alternatively, calls may be recorded and the recorded data used for input. Off-line receivers may call back their network or may record incoming calls to ensure that incoming wires were properly received.

**Data Entry.** If data are to be manually entered into a terminal, it can be useful to require that all transfers be entered twice or to have a second operator independently verify the entry to ensure against operator errors. If this is done, transfers should not be released unless all data in the two entries match. Software controls should also be in place to guard against the inadvertent release of a duplicate transfer.

**Minimization of Manual Intervention.** The American Bankers Association's publication *Developing a More Efficient Funds Transfer Service: Phase II* provides network formatting conventions and internetwork conversion rules that will facilitate the processing of funds transfers between networks, all of which have different format standards. The publication also provides standards to facilitate the posting of entries to a customer's account. The minimization of manual handling not only offers the obvious operational benefits, but also reduces the risk of operational error. The use of an automated recurring transfer file for frequently made transfers can also reduce the amount of operator intervention.

**Deposit Deadlines.** All fund transfer networks have preset close-off hours that are usually extended only on an emergency basis. In addition, the nature of funds transfer activity is such that peaking generally occurs in the late afternoon, immediately before the network's close-off time. Because of this peaking, a bank should allow ample time between its deadlines to its customers and the network deadline for the bank to ensure that it can effect the message, settle its position, and handle required customer notification. As with any activity, errors are most likely to be

made when time pressures are most acute. For this reason a bank must balance the needs of its customers for the latest deposit deadline against its capacity to handle the transfer in a timely and accurate manner.

**Software Development and Testing.** Because of the high risks in funds transfer, it is vital that any software be adequately and thoroughly tested before being used. Even minor program changes should be tested with several days' data to ensure accuracy.

**Account Reconciliation.** As with fraud risk, account reconciliation may not enable a bank to keep an error from happening; but the longer a bank waits to detect an error, the more difficulty it will have recovering, as the funds get drawn down by the recipient.

**Use of Suspense Accounts.** When operational errors do occur, many banks will quickly adjust the accounts of their customers and put the offset into a "suspense" account pending final resolution. While this procedure is good for customer relations, suspense accounts should be monitored and followed up quickly to avoid a loss.

A bank cannot possibly have a 100 percent guarantee against operational error. However, an on-going program can reduce the potential for operating loss by ensuring that—

- ~~Staff is properly screened before being hired~~ (for example, by extensive checking of references and exhaustive credit checks) ~~and is trained~~ in both the operational and security aspects of the job;
- ~~Job standards, quality control program, procedures documentation,~~ and proper lines of supervision are in existence;
- ~~Special supervisory attention is given to~~ high dollar or nonroutine transfers; and
- ~~automation is used as much as is feasible~~ (because operator or clerical error represents the single most prevalent reason for loss within payments systems).

Within and between many clearinghouses, rules have been established for settling compensation claims arising from interbank payment errors. Developed by the Nationwide Task Force on Uniform Compensation, these rules generally govern compensation for lost availability but do not apply to the recovery of lost principal. The purpose of the rules is to avoid undue injury or unjust enrichment to one party as a result of an error by another party. The rules also promote the prompt and orderly submission of claims and provide incentives for the prompt return of funds sent in error. A copy of the proposed compensation claim rules is included in Appendix 2 and can serve as a model for dealing with interbank compensation claims or claims between a bank and its customer.

## FRAUD RISK

Fraud risk, like operational risk, is any act that causes a bank or its customer to lose money, goods, or services, but in the case of fraud risk the act is intentional instead of inadvertent. Four major types of fraud risk must be guarded against:

- initiation of a fraudulent transfer request;
- alteration of the terms (either the amount or the beneficiary) of a valid request;
- purposeful destruction of records resulting in the erasure of a valid transfer; and
- inadvertent alteration, misdirection, or duplication that results in an unauthorized recipient's absconding with the funds.

Because funds transfers are generally irrevocable, any fraudulent transfers may have to be covered by the originating bank.

Although the average funds transfer is in excess of \$2 million, such transfers are not likely to be scrutinized any more carefully than transfers of lower dollar values. For this reason, controls must be in place to

guard against the possibility of unauthorized access to the funds transfer network and to ensure that personnel with authorized access do not have an opportunity to enter fraudulent transfers.

Although fraud loss may be perceived as the largest funds transfer risk, the banking industry apparently has no comprehensive data on the frequency, size, or type of fraud losses, nor have many cases of fraud or other corporate EFT risk been documented. This is partly because, fortunately, there have not been that many instances of major payments system losses. Yet the risk of fraud loss is clearly large because of the high dollar value transferred. Furthermore, the risk appears to be increasing, partly because of the greater number of funds transfer participants and the public's increased knowledge of computers.

To diminish the risk of fraud, four distinct control points must be addressed:

- between the originating company or correspondent bank and the bank entering the transfer into the wire network;
- between the originating bank and the network;
- between the network and the receiving bank; and
- between the receiving bank and its corporate or correspondent bank customer.

The vulnerability to fraud does not appear to differ markedly by type of network, so in what follows the various wholesale electronic payments systems will not be treated separately.

The primary fraud control objective is to ensure that transfers are authorized. Although no one method can be 100 percent effective, several common techniques are used to guard against unauthorized transfers:

**Authentication Codes.** The most common method used to ensure authorized access is the use of authentication codes. Most wire networks supply the originators

with a unique sequence of codes that are to be entered with each transfer. The receiver of the transfer can verify the authenticity of the sender by matching the code sent with the transfer to the receiver's code list.

Code authorization should be used not only between the bank originator and the network, but also between the bank and its corporate or respondent originators. Codes should be used for both on-line and off-line access.

Although at present codes need not be used for ACH transactions, some method of authorization (e.g., signature verification of tape transmittal documents, and logging procedures) should be used.

Merely having a code system does not guarantee against the risk of fraudulent input. Tight controls must be in place to ensure that these preassigned codes are not available to parties other than those authorized to originate transfers. Banks can significantly lessen their risk by ensuring that authentication codes are not taped to terminals or desks or left out for others to see. When distributing codes to customers, one should make such distribution directly to the appropriate party in a confidential manner, such as by registered mail or messenger. To reduce on-going risk and risk associated with a departing employee, techniques such as frequently changing the codes or changing them with each transfer can be used.

**Call-Back.** Some wire networks will use a call-back system to ensure that the transfer request comes from an authorized source. Under this procedure, the receiver of the transfer instruction will call back the institution that requested the transfer (using a list of preauthorized telephone numbers) to verify the validity of the source of the request. This is a control against the possibility that an outside party who has access to the authorized codes will fraudulently make a transfer request. Despite the time and expense involved in the call-back procedure, it is a good way to verify that the initiator of the message was in fact who he or she purported to be. The call-back is

often made to a party other than the initiator of the transfer, to minimize the risk of an initial call being unauthorized.

The call-back procedure can be used not only between an off-line bank originator and its funds transfer network, but also between the corporate or correspondent bank originator and its bank and for the receipt of incoming transfers. Since the use of proper authentication codes does not guarantee that such codes were not obtained by outside parties through fraudulent means, a call-back procedure will at least verify the authenticity of the calling party.

An analogous procedure can be used for on-line institutions. If each terminal has unique identifiers or passwords, the terminal identifier can then be used to verify that the input terminal has been authorized to send payment instructions. This reduces the risk that unauthorized parties will tap into the network.

**On-Line Access.** Terminal access rather than phone-call access not only provides the opportunity for reducing costs for medium- to high-volume traffic; it also generally provides better opportunities for integrating security features into a funds transfer system. Both hardware and software security features can be incorporated into an on-line funds transfer connection, for a bank's dealings with both its funds transfer network and its customers.

**Wire Room Security.** For control all of these methods presumably have to do with fraud control against destruction of records and equipment or initiation of invalid transfers, tight security of wire rooms is essential. If possible, the facilities used for entering transfers should be subject to restricted access, and personnel employed in the wire room should be screened before employment and well trained in the security aspects of their jobs. Incoming and outgoing phone calls can be tape recorded, to provide an audit trail if a fraudulent transfer does occur.

Wire room security should also be extended to the software programs used by

on-line banks and customers of banks who are also on line. This security should not extend only to live software, but also to back-up software and all development efforts for wire transfer software.

**Special Security Program Edits.** For both on-line and off-line institutions, special security software edits can be applied. Dollar value limits can be established for each customer, governing the size of an individual funds transfer or the aggregate value of transfers made by a single customer. Transfers above these amounts can be either automatically rejected (at the customer's request) or referred to a supervisor for approval or call back to the originating party.

A recurring transfer file can also be established for transfers that are common as to beneficiary or beneficiary and amount. The use of a recurring transfer file reduces the risk that the intended third-party beneficiary will be inadvertently altered.

**Reconciliation.** Wire transfer records received from the network should be reconciled daily. Although this in itself will not reduce the prospect of fraud, the more quickly any fraud is discovered, the more chance a bank has of recovering the funds.

**Data Encryption.** Data encryption is a security measure that can reduce the risk of unauthorized monitoring or tampering with messages. While at this time highly sophisticated data encryption may be cost effective only for the largest institutions, simple encryption techniques, such as letter substitution, can be reasonably inexpensive. Such simple techniques can be used for on-line communications between a bank and its correspondent or corporate customers, to reduce the opportunities for monitoring or fraudulently altering data.

To ensure that security measures, once developed, are maintained, an ongoing security maintenance program should be in place in all banks. This program entails the following:

- Documentation of security procedures for each point of control (customer to originating bank; originating bank to network; network to receiving bank; receiving bank to customer).
- Assignment of a bank officer to be responsible for wire room security. This individual should have special knowledge of hardware and software as this is necessary for effectively managing the security program connected with funds transfers.
- Frequent reviews by the audit staff of both the written procedures and procedure compliance.
- Standardization and frequent review of customer legal agreements.

To transfer the remaining fraud risk, a bank should consider legal agreements (which are discussed in greater detail below). Each bank should have legal agreements with each of its customers spelling out the responsibilities and liabilities of each party. Because there are few laws relating to wire transfer activity, a properly prepared legal agreement may be a bank's best protection against fraud caused by other than bank employees.

The following case studies<sup>1</sup> illustrate methods that have been used to try to obtain funds fraudulently.

#### Case 1

A major money-center bank hired an outside vendor to develop and implement a new funds transfer system. Several weeks after the system was accepted, an employee of the vendor returned to the wire room, ostensibly to conduct a "post-implementation test" of the system. Sometime later it was discovered that an unauthorized transfer in excess of \$10 million had been made from the money-center bank to a Swiss account via a New York bank.

<sup>1</sup>Because much of what is learned about payments system losses comes third-hand and from rumor and speculation, the author wishes to apologize in advance if any factual distortion of the cases exist.

There are, of course, several morals to this story. First, access to secured areas must be tightly controlled. People without specific authorization should not be allowed to enter wire rooms, even if they have been seen there before.

Second, passwords are useless if they are available to people other than those specifically authorized. Authorization code words and other security access systems must not be left where nonauthorized personnel can find them.

## Case 2

Some years back, an individual placed several calls to both Federal Reserve and commercial bank wire rooms to find out more about how funds transfers were effected and what people (by name) were employed in the Federal Reserve and commercial bank wire rooms. After amassing whatever information he could, the individual called several commercial banks in the area, claiming to be from the Federal Reserve wire transfer department and making an incoming third-party transfer to the account of a customer of the bank. When the individual showed up to claim the money at one of the banks, he was met by police (who had been notified by the bank) and was arrested. When put into jail, the individual used his one phone call to try to initiate a "FedWire" transfer into his account—demonstrating, perhaps, the perseverance of those who attempt EFT fraud. As with the first case, the incident is instructive in several ways.

When nonauthorized people ask questions about wire room procedures, **be alert and alert others**. One of the main reasons the individual was stopped was that the commercial banks called by the perpetrator recognized a potential problem and notified the Federal Reserve; the flurry of phone calls (all made under different names) alerted the Fed that something was brewing. The Fed, in turn, notified all funds transfer customers to be alert for some form of fraud action.

**Pay attention to all elements of the funds transfer activity.** It is commonly thought that funds transfer is most vulnerable to fraud or operator error at the originating end and that once a bank is notified by the "Federal Reserve" of an incoming transfer, the transfer is irrevocable. On the contrary, a fraudulent transfer can be entered at any point along the funds flow system, and in many ways, the later in the funds transfer process the fraudulent transfer is entered, the less likely it is to be discovered.

## CREDIT RISK

Perhaps the least understood and therefore least monitored risk is the credit exposure associated with funds transfer systems. Because funds transfers are generally both immediate and irrevocable, when a funds transfer is made, the bank originating the transfer is in essence guaranteeing the credit of the customer that has requested the transfer (and, in some cases, guaranteeing the credit of the bank that transfers the money). Unlike the check system, in which a check can be returned if the writer has insufficient funds, once a bank releases a wire transfer, it is guaranteeing that the funds will be paid. If the customer that authorized the transfer cannot pay, then the bank must do so.

For this reason, the transfer of funds should be looked upon as analogous to the authorization of a loan. Therefore, systems should be in place so that the bank knows whether the loan is made on a secured or unsecured basis—knows, that is, whether the originator has available the funds or collateral to cover the transfer.

The failure to deal properly with credit risk can lead to the loss of principal for the entire amount of the transfer or for the amount over and above the customer's funds on hand.

Credit risk exposure, then, occurs whenever a bank releases funds without having collected funds to draw against. This credit

risk exposure can always exist for the originating bank and may exist for the receiving bank as well, depending on the network used to transfer the funds. Because much work on the issue of credit exposure is being done by the funds transfer networks themselves, their activities are discussed below, followed by a discussion of techniques for minimizing credit risk.

## **FedWire**

The Federal Reserve's communications systems (FedWire) is the only truly instantaneous, irrevocable settlement system. Funds received via FedWire are guaranteed good funds to the recipient. Therefore, the recipient has no credit risk when passing those funds to its customer.

The Federal Reserve, however, in passing irrevocable funds to the receiving bank, incurs the risk that the sending bank will be unable to cover the transfer. This risk could be reduced if the Federal Reserve had an on-line accounting system enabling it to know whether the originating bank had sufficient funds in its reserve account to cover the transfer. At the present, however, Federal Reserve Banks lack the real-time accounting system necessary to know whether sufficient funds do exist in the originating bank's reserve account. Instead, the Fed relies on its knowledge of the financial condition of banks as well as on after-the-fact monitoring of and counseling on intraday overdrafts to control its degree of risk exposure.

Even if the Fed becomes capable of monitoring the condition of each bank's reserve position on a real-time basis, it would probably not reject all transfers that would leave a bank in an intraday overdraft position. It is generally agreed that the smooth functioning of the payments system requires some extension of credit to avoid creating the problems that will inevitably occur if each bank waits until just before the FedWire close-off to initiate outgoing wires, thus maintaining a high reserve position as long as possible.

In the absence of an absolute prohibition against intraday overdrafts, the Fed will probably look to one or more of the following methods for limiting *its own* credit exposure:

- developing an on-line, real-time accounting system to track the collected funds in each bank's reserve or clearing account;
- setting intraday overdraft limits based upon the perceived credit-worthiness of each customer;
- requiring collateralization of all daylight overdrafts; and
- establishing caps on the total amount of credit exposure equal to some multiple of a bank's capital.

Each of these methods has some advantages and disadvantages, and when the Fed has a real-time accounting capability, possibly some combination (e.g., a credit cap with collateralization beyond the cap) will be used.

In theory, the use of intraday limits based upon the credit-worthiness of each institution is probably the best way to truly minimize risk exposure. However, this would require the Fed to make what might seem arbitrary decisions regarding the credit risk of individual participants. Given the large number of FedWire participants, the application of this process to all institutions would be cumbersome and subject to dispute.

Collateralization of *all* daylight overdrafts would not be feasible for many organizations. Because of the high volume of funds transfers, a bank may often have daylight overdrafts far in excess of its available collateral. Further, collateralization does not serve to reduce the overall risk but merely transfers it from the Fed to the banking industry—a situation, given the Federal Reserve's regulatory role, which may not be attractive to the Fed.

Intraday credit caps, if set too high, will not reduce payments risk. However, if set

too low, they could cause network gridlock: the potential for a rejection of transfer activity due to the credit caps could cause many banks to hold outgoing transfers to the end of the day, which would cause other banks, expecting incoming transfers, to approach their credit cap.

## **CHIPS**

CHIPS payments are not final when initiated, but are settled at the end of the day through a net settlement arrangement with the Federal Reserve Bank of New York. During the course of the day, CHIPS accumulates the net position of each CHIPS settlement participant. At the end of the day, each bank with a net debit position will wire funds to cover its debit to the CHIPS account in the New York Fed. Once all incoming transfers have been received, CHIPS wires funds out of the account to cover each bank with a net credit position.

If a bank cannot cover its net debit position or if one of the settling banks cannot cover a debit position held by one of its correspondents, CHIPS rules call for the entire settlement to be "unwound" and a new position calculated for each bank, netting out all the activity of the nonsettling participant. Theoretically, this unwinding process could leave another bank in a position where it could not cover its debit, leading to a further unwinding.

As a practical matter, because of the very real potential for a chain of failures arising from the unwinding of a settlement, an unwinding of a CHIPS settlement will probably never take place; or it will take place only as a last resort. Nevertheless, since CHIPS payments are not final until settlement takes place at the end of the day, any release of funds received via CHIPS before end-of-day constitutes the release of technically uncollected funds and represents a credit risk to the releasing bank.

To minimize the risk of having to unwind a settlement, CHIPS is considering measures limiting credit risk, such as bilateral credit arrangements or a cap (both of which are used for CashWire, see below).

## **CashWire**

Like CHIPS, CashWire does not provide for immediate settlement. The physical process of CashWire settlement takes place at the end of the day in a manner very similar to CHIPS settlements, but the settlement is not final until 9:00 A.M. the next day. The delay in finality of settlement until 9 A.M. coupled with provisions in CashWire for finality of credit to customers gives rise to receiver risk. To control receiver risk, BankWire's CashWire service incorporates two principle features.

With a bilateral credit limit, each bank establishes for every other bank with which they choose to exchange CashWires, a credit limit which limits the bank's credit exposure. The credit limits are based upon the degree of credit risk each bank is willing to accept for each other bank. Too high a limit may lead to too great a credit exposure, while too low a limit may cause otherwise valid wires to be rejected too often. Each bank can adjust its limits during the day if too many transfers are being rejected or to limit the number received.

In addition to bilateral limits, CashWire also has an aggregate debit cap for each participant. This is to avoid the possibility of a bank being overextended in total while still being under each of the separate bilateral caps. The current CashWire cap is set at 50 percent of each bank's capital.

Because a CashWire settlement is not final until 9 A.M. the next day, a receiving bank assumes a credit exposure since it releases funds to a customer before that time. However, the use of bilateral limits and aggregate credit caps somewhat reduces that risk.

## **Techniques for Minimizing Credit Risk**

The networks' attention to credit risk and the methods they use in treating it should be instructive to all funds transfer users trying to manage the credit risk between the originating and receiving banks and their customer. In particular, to reduce their

credit risk, originating banks can take the actions prescribed below.

**On-Line Accounting System.** If feasible, a bank can develop an on-line accounting system enabling it to track the large dollar deposit and withdrawal activities of major funds transfer users. The system should, if possible, distinguish between collected and uncollected funds and should, at a minimum, accumulate all funds transfer activity throughout the day. If a corporation has multiple accounts, these accounts should be aggregated. The funds transfer system should then be able to reject or hold transfers based upon the condition of the customer's balance.

**Upper Credit Limit.** To retain good customer relationships, it may not be desirable to reject any transfer that places a customer in an intraday overdraft position. However, some upper credit limit should be established with each customer so that a bank can, as a minimum, make a conscious decision whether to honor any transfers that will leave a customer above that limit. The establishment of these credit limits should be managed like any other bank credit decisions and should involve the bank's lending officers, correspondent bank officers (for correspondent banks using funds transfer), and the credit committee.

**On-Site Collateral.** If credit limits alone do not enable a bank to balance its needs for limiting credit exposure against a customer's payment transfer needs, a bank should consider requesting on-site collateral as a means of controlling credit exposure.

**Legal Agreement.** The legal agreement for funds transfer should have provisions covering the bank to the fullest extent possible in the event of a customer's inability to fully cover an overdraft.

Receivers, too, should be cognizant of the risk they incur in passing uncollected funds to their customers. As is noted above, this is not a problem in FedWire but could be a problem in CHIPS and CashWire.

Again, banks can and should establish some form of credit limit for extending immediate-use funds to their corporate or correspondent bank customers for incoming CHIPS and CashWire transfers.

Because each of the three funds transfer networks is considering some form of credit risk control (either bilateral agreements or credit caps), banks should begin to involve their credit people in the credit risk control process. Bank credit officers should begin *now* to familiarize themselves with the funds transfer activity of their corporate and correspondent customers and with the funds transfer volume received from other banks so that they will be able to make intelligent credit decisions if (and more likely when) credit controls are applied to the major funds transfer networks.

To develop the data for predicting what might happen should all funds transfer systems place a cap on the level of intraday credit exposure they will accept, each bank should track funds transfer inflows and outflows by source. Analyzing traffic patterns and involving the credit department in the analysis of the credit-worthiness of a bank's frequent funds transfer trading partners will be time-consuming. If the bank leaves too little lead time, it may find itself setting limits either too high, which may yield a credit risk exposure beyond what is acceptable, or too low, which may lead to frequent rejections of funds transfers, thus impairing customer relations.

## RISK OF SERVICE DISRUPTION

Because banks routinely transfer tremendous sums of money daily, any disruption of service due to power outages, computer failures, natural disasters, etc., can be devastating. While banks have recently been paying more attention to contingency backup facilities, the mere acquisition of such a facility does not guarantee that it

can be used in a timely manner when a service disruption occurs in the main processing cycle. For that reason, funds transfer managers must be prepared to use a variety of contingency backup modes for rapid restarting.

In general, liability for service disruption is limited to the loss of earnings on the funds during the delay, but conceivably a delayed transfer could lead to consequential damages, particularly if a bank does not have reasonable backup procedures. In addition, too great a frequency of service disruptions could certainly lead to customer dissatisfaction and loss of business.

To minimize the risk of service disruption, a bank can take several steps. The most significant is arranging an off-site backup facility for occasions of major and lengthy service disruption (e.g., after fire, flood, etc.). But because much work is being done on disaster planning, this study does not discuss off-site backup. Rather, it concentrates on less comprehensive, less expensive, but perhaps more timely means of backup for the more common outages of relatively short duration (one day or less).

**Duplication of Facilities.** Large funds transfer users should consider having redundant processors, lines, terminals, and software in the event of an outage of the main unit. Redundant processors, however, may be an adequate backup only if the bank also maintains a mirror image of the day's processing activity, codes, etc., to allow for quick switching of the processors.

**Alternative Network Capability.** A large institution should also consider membership in multiple networks, so that the inability to access one network, through either internal or network failure, will not cause a complete stopping of funds transfer activity.

**Trained Backup Staff and Emergency Procedures.** In the event of a failure of an on-line institution's computer and terminal equipment, that institution can continue to function for at least some of its transfers in an off-line mode. This requires an adequate standby staff of trained individuals who can initiate transfers via telephone. Sufficient staff should be selected and trained to ensure the reasonably smooth continuation of service, and backup manual procedures should be well documented. Backup staff should be used periodically in the funds transfer area to ensure their familiarity with the function.

In addition, the bank will probably need some system of prioritizing, either by dollar amount per customer or by type (third party vs. self), to ensure that transfers not able to be effected on a timely basis are of lower priority.

In addition to providing some degree of backup capability, *banks should realize that when operating in a contingency mode, they are most vulnerable to other types of risk, such as fraud, operating error, and credit risk.* For this reason, contingency operations should be well documented and subject to extra supervision.

# CHAPTER THREE

## Risk Control and Risk Transfer

### RISK CONTROL

Once a bank has identified the risks associated with wholesale EFT, it should establish an ongoing risk control program that includes continuous monitoring and updating. The goals of the program are:

- to identify the actions and costs necessary to eliminate the risk exposure or at least reduce it to a tolerable level; and
- to ensure that the risk control procedures are being followed.

To achieve these goals, internal responsibility for risk control for corporate EFT should be clearly assigned. The individual or individuals chosen should be knowledgeable about corporate EFT operations and systems. They should also be at a high enough level in the organization to command the resources necessary for managing risk control and to identify to senior management the vulnerabilities and the costs of reducing the vulnerabilities.

Those responsible for corporate EFT risk control should also be a part of any process of developing or modifying products or systems from the inception of the process. Making control procedures a basic part of the system design is almost always less expensive and more effective than trying to retrofit control measures after the fact.

Finally, the potential for loss in corporate EFT is such that it should command the ongoing attention of a bank's senior management. Reports on operating errors,

corporate EFT losses, investments needed for control, etc., are best brought to senior management attention on a regular basis to ensure understanding and support for the risk control effort throughout the organization.

### RISK TRANSFER

#### Insurance

Thus far, this paper has dealt primarily with identifying and controlling risk. As has been noted, it is virtually impossible (or at least cost prohibitive) to eliminate 100 percent of payment system risk. Because the loss exposure is potentially so high, banks must have some method of transferring the risk to others, primarily through insurance. Insurance, however, should not be the first line of defense against payments systems risk, but the last. A risk assessment may be required by the insurance company before providing coverage. This is because a bank's premiums will be affected by the quality of its risk control program; and with an inadequate program, the bank may be unable to obtain coverage or may have to assume a greater portion of the loss through a larger deductible.

Furthermore, the real purpose of insurance for payments systems risk should be to cover very large and, it is hoped, very infrequent losses. Insurance should generally not be used to cover small-dollar-value losses that can be absorbed internally, probably at a cost far lower than insurance

costs. Therefore, a bank should seriously consider a reasonable deductible level in its policy and use the savings in premiums to partially fund the risk control program and small-dollar-value losses.

The bankers blanket bond provides coverage for a wire transfer if the transfer results in a fidelity loss caused by officers, employees, independent contractors, or others in collusion with officers and employees. In addition, the on-premises coverage of the blanket bond applies if there is manipulation of the bank equipment on premises by independent contractors or persons other than officers or employees. And through the computer systems rider of the blanket bond or through a separate electronic and computer crime policy, banks can purchase coverage for loss due to an interloper which is an illegal attack against the security of EFT systems such as BankWire, FedWire, SWIFT, and CHIPS, systems operated by individual automated clearinghouses, ATMs, bank proprietary systems, or any other computer system.

If there is no fraud, forgery, or employee dishonesty, the loss is covered only if the bank has a bankers professional liability policy, and then only if there is third-party liability. The professional liability policy covers the bank for any damages that result from any act, error, or omission committed or alleged to have been committed in the rendering of professional services. The term "professional services" is broadly defined to mean services performed by the bank for any customer or client. The bank's risk and insurance management department or insurance officer can help analyze this aspect of risk transfer.

The types of coverages applicable to corporate EFT are now changing. For example, about a year ago a new computer systems rider was made available to cover against loss caused by fraudulent entry of data into, or fraudulent change of data elements or programs within, a computer system. In addition, some insurance companies have recently revised their coverage

to provide broader protection for the risks of electronic banking.

As EFT evolves, probably insurance coverage will evolve also. For this reason, it is important that a bank review its electronic and computer crime coverage periodically to make sure that its insurance needs are being met.

## Legal Agreements

A second method of transferring risk is through a legal agreement with the customer. *Because there is no formalized law covering wholesale electronic funds transfer, a major source of the bank's legal protection is a legal agreement detailing the specific rights and responsibilities of all parties.* Obviously, a bank would like to place as much risk as possible on the customer, who in turn would like to see the bank absorb all the risk.

From a bank's perspective, it is probably not realistic to assume that the customers will be willing to absorb more than their full share of risk. Many banks offer funds transfer services, and if a bank's legal agreement appears overly burdensome, its customers just might go elsewhere. Beyond that, the absence of an accepted payments code of law for funds transfer will probably cause most questions of large dollar liability to go through the courts, and if a bank's legal agreement provides for the unreasonable transfer of risk to its customer, the court may rule against the bank even if the legal agreement specified the customer as liable.

For these reasons, care must be taken in developing a funds transfer legal agreement such that a bank accepts what liability it can rightfully control and passes on to customers what is controllable by them or not controllable by either party (e.g., acts of God—floods, earthquakes, etc.).

Accordingly, a bank's legal agreement should accept liability for its own negligent performance or nonperformance of agreed upon responsibilities and should accept responsibility not only for loss of principal but also for loss of interest due to nonper-

formance. However, the legal agreement should exempt the bank from liability for the customer's failure to use and/or protect security codes and failure to take other security measures that should be described in the agreement.<sup>2</sup> Further, the legal agreement should (a) limit the period of time during which a customer can make a claim, (b) define the bank's right to refuse to honor a transfer that would lead to an overdraft, and (c) define the customer's obligations and responsibilities if an overdraft does occur. Finally, the bank should specifically exempt itself from liability for any consequential damages that might arise, recognizing that ultimately a court may decide such issues on a case-by-case basis irrespective of the language in the legal agreement.

The legal agreement should be reviewed periodically, generally on a fixed review cycle so that the process is institutionalized. The reviews would ensure that the legal agreements are kept current.

Like insurance, a legal agreement is necessary to protect a bank against undue risk. However, like insurance, a legal agreement should not be viewed as absolute protection against all forms of payments systems risk. The legal agreement serves only to limit the risk to areas within a bank's control, but does not eliminate the need for a good risk control program.

### **Charges to the Customer**

A third commonly used method of risk transfer is to build some allowance for risk into the price charged for the service. It is not practical to build all payments systems risk into the price charged for funds transfer, because good information on the frequency of such risk is lacking and because the potential for loss if a major problem should occur is almost unlimited. Beyond that, it is highly unlikely that cus-

<sup>2</sup>In this report, the risk control focus has largely been on the bank. However, a bank can reduce its own risks and provide a better service to its customers if it provides information and systems to help its customers control their risks.

tomers will be willing to pay very much for payments systems risk, since most banks will not build that payment into their prices.

However, what banks probably can build into their service price structure is coverage for the cost of their risk control effort, since a good risk control program protects both the bank and its customer. Further, banks should try to build into their prices some allowance for small losses that might occur—those under the deductible level of the insurance coverage.

In the final analysis, an effective risk control program, although it can be expensive, will probably lead to lower, rather than higher, long-term costs and therefore a lower rather than a higher price. Losses will be minimized and controls will generally be implemented in a more cost-effective manner.

## **FUTURE RISK CONTROL**

It is not clear that, on balance, the future will see a significant reduction in payments systems risk. Changing technology will probably serve to reduce risk in some areas but increase it in others. In a few years, improvements in data encryption technology may lead to cost-effective techniques for data encryption of funds transfer messages, reducing the possibility of fraud through unauthorized tampering with or monitoring of messages. In addition, the lower cost of terminals will enable more banks to be on-line to their funds transfer network, and more customers to be on-line to their banks. An increase in on-line connections will reduce the greater risk of fraud and operational error for off-line service.

On the other hand, improvements in technology will enable more banks and corporations to avail themselves of funds transfer service, and as less experienced participants become involved, the risks of fraud, operator error, and credit risk all increase. Moreover, as the knowledge of computer technology reaches almost every household, the prospect of funds transfer

tampering by outside parties increases. The number of white collar bank crimes (embezzlement and record alteration) already exceeds the number of bank robberies by a significant margin, according to current estimates. As people are increasingly exposed to computer technology, the prospect of computer crime increases.

Because of the increased awareness of payments systems risk, attempts are likely to be made to limit the risks or quantify them better. Because these attempts are still very much in their infancy, only two are discussed below.

### **Federal Reserve's Attempts to Limit Risk**

The Federal Reserve is not only active in funds transfer through FedWire, but it also provides net settlement services for Cash-Wire and CHIPS and, as a banking regulator, has a role in ensuring the safety and soundness of the banking industry. For these reasons, and because of the dramatic expansion in the number of FedWire participants due to the open-access provisions of the Monetary Control Act, the Federal Reserve has become very concerned about the credit risk undertaken by the various wire networks.

At present, the Federal Reserve tries to minimize that risk by imposing penalties for overnight overdrafts and conducting "ex-post" monitoring and counseling to control intraday overdrafts. Apparently these actions do not eliminate as much of the credit risk as the Fed would like, partly because the Fed lacks the capability to do

real-time monitoring of daylight overdrafts and partly because, in the absence of similar credit controls on all funds transfer networks, banks can avoid FedWire credit restrictions merely by using another network.

It is therefore likely that over the next few years, the Federal Reserve will consider some method of reducing the banking industry credit risk, irrespective of whether transfers occur over FedWire or over a system that uses the Federal Reserve's net settlement system. The methods most likely to be considered are—

- establishing a credit cap for a bank's participation in all networks, either on a bank-by-bank basis or with a standard limit equal to some multiple of a bank's capital; and requiring each bank to pre-allocate its credit limit to the various funds transfer networks; and
- requiring collateralization of all intraday overdrafts or those intraday overdrafts that are above the credit cap.

In addition to credit risk, fraud, operational, and service disruption risks have long concerned the Federal Reserve as well. In late 1984 or early 1985, the Federal Reserve is expected to implement a new standard funds-transfer and communication system that is expected to provide, among other things, better security, message accountability, and backup capability.

As the date for implementing these changes nears, Federal Reserve personnel will no doubt be informing FedWire users of the changes in the Federal Reserve fund transfer system.

# CHAPTER FOUR

## Summary and Conclusions

This study has identified the major areas of risk in wholesale electronic payments systems, with particular emphasis on steps that can be taken to reduce those risks. Because wire room operations differ from bank to bank, there is no single process that every bank can go through to minimize its risk, nor can any bank guarantee an absence of exposure to loss.

However, through an effective program of risk identification and control coupled with an ongoing administration program, a bank can reduce the risk of loss and embarrassment. By following some of the suggestions in this paper, a bank can make a start in that direction. *One effective way of developing and continually improving a bank's risk management program is to compare the control concepts used by the bank's funds transfer network supplier (FedWire, CHIPS, CashWire) to its own internal operations and its customer interfaces.* The survival of these networks depends on their having sophisticated risk control programs, which they have therefore spent significant amounts of time and energy in developing. These operators would be happy to share some of their risk control concepts with the bank, and the bank can look to their knowledge and experiences as an excellent starting point for either developing or enhancing its program.

In addition, if a bank has not done so already, it should begin to analyze the degree of credit risk being absorbed daily through its wire room activities. Although attention to such traditional risks as fraud and operating errors should not be minimized, the major risk focus over the next

several years is very likely to be credit risk. The sooner a bank begins to involve its credit department and account managers in the process of reviewing payments credit risk, the more likely the bank is to develop a program that balances credit risk against the smooth functioning of its wholesale EFT payments systems.

It is highly unlikely that any bank can take measures to completely eliminate risk in wholesale EFT. It is therefore necessary for a bank to have adequate insurance coverage and legal protection to limit its losses if fraud or operating error should occur. Because the use of corporate EFT is rapidly expanding, both the types of insurance coverage available and the legal framework for corporate EFT are likely to change over time, which means that for a risk transfer program to be effective, not only must insurance and legal agreements exist, but they must also be periodically reviewed.

Although a successful risk control program can take many forms, certain elements appear to be vital for success:

- The program must not only include a one-time assessment of risk, but should also incorporate periodic reviews to evaluate how risks, or procedures to guard against the risk, change over time.
- While the program should focus on methods and procedures for minimizing risk, it should not ignore the need for transferring risk, such as through insurance and legal agreements.
- Overall responsibility for risk control should be clearly assigned within the

organization to provide coordination across organizational units.

- Although responsibility should be directed at particular units within the bank, the nature of the risks in corporate EFT are such that an effective program must cross many organizational lines. Therefore, virtually everyone in the bank should be aware of the vulnerabilities in corporate EFT and of his or her responsibility for minimizing such risks.

The relatively low incidence of loss in corporate EFT to date is testimony to the fact that controls, if properly developed and maintained, can minimize the prospect of loss even in high-volume, high-value payments systems. However, because of the changing magnitude and nature of corporate EFT risk, continuous review and updates of existing risk controls are necessary if the low incidence of loss is to continue.

# APPENDIX 1

## Sample Checklist of Major Vulnerabilities, Control Procedures, and Organizational Responsibilities

This appendix presents a sample checklist that identifies some of the major vulnerabilities of wholesale electronic payments systems, control procedures to minimize the risks, and organizational responsibilities. Since each bank is likely to have its own unique operating characteristics and organizational structure, any

universal checklist would be incomplete, so this sample should be used only as a guide for a bank in creating its own checklist. Not only should a checklist be created, but each party with some control responsibility should have a copy of the relevant section of it.

### SAMPLE RISK CONTROL CHECKLIST

VULNERABILITY	TYPE OF RISK EXPOSURE	PAGE ON WHICH DESCRIBED*	SUGGESTED CONTROL STEPS	RESPONSIBILITY
1. Unauthorized access to wire room	• Fraud	11	<ul style="list-style-type: none"> <li>• Restrict access to area via                             <ul style="list-style-type: none"> <li>—card or code-controlled access</li> <li>—partitioning</li> <li>—guards</li> </ul> </li> <li>• Training of employees to question outsider authorization</li> </ul>	Security Officer
	• Sabotage leading to service disruption	17		Security Officer/ Operating Officer
2. Unauthorized access to telephone or terminal	• Fraud	12	<ul style="list-style-type: none"> <li>• Use of authentication codes</li> <li>• Call-back</li> <li>• Legal Agreements</li> </ul>	Operating Officer Operating Officer Legal Department
3. Control of authentication codes	• Fraud	11	<ul style="list-style-type: none"> <li>• Training of employees to control codes</li> <li>• Supervisor review of controls</li> <li>• Call-back verification</li> <li>• Legal agreements</li> </ul>	Operating Officer   Legal Department

\*Page in this report that describes the risk more fully.

107

**SAMPLE RISK CONTROL CHECKLIST (Continued)**

VULNERABILITY	TYPE OF RISK EXPOSURE	PAGE ON WHICH DESCRIBED*	SUGGESTED CONTROL STEPS	RESPONSIBILITY
4. Operating error leading to potential for fraud	• Fraud	11	• Verification before release	Operating Officer
			• Call-back	Operating Officer
			• Training	Operating Officer/ Personnel
			• Recruitment security check	Operating Officer/ Personnel/ Security Officer
			• Software edit checks, e.g., as to dollar amount or third party	Operating Officer/ DP Officer/ EDP Audit
	• Procedures manuals		Operating Officer/ Audit Dept.	
5. Error allowed to "age"	• Fraud	11	• Daily reconciliation of statements	Operating Officer
	• Operating loss	9	• Daily reconciliation of suspense accounts	Operating Officer/ Audit Dept.
6. Data entry error	• Fraud • Operating loss	11	• Operator training	Operating Officer
			• Verification	
		9	• Call-back	
			• Software edits • Call recording	
7. Failure to enter transfers	• Operating loss	9	• Operator training	Operating Officer
			• Logging and balancing of transfers	
			• Allowing sufficient time before deadlines	
			• Staffing and back-up procedures	
8. Extension of credit to corporate or correspondent customer	• Credit exposure	14	• On-line accounting system to monitor credit exposure	Accounting Officer
			• Establishment of credit lines	Credit Officer/ Account Manager
			• Establishment of collateral	Credit Officer/ Account Manager
			• Automated controls to hold transfers beyond credit limit	DP or Operating Officer
			• Legal agreements	Legal Department

\*Page in this report that describes risk more fully.

108

### SAMPLE RISK CONTROL CHECKLIST (Continued)

VULNERABILITY	TYPE OF RISK EXPOSURE	PAGE ON WHICH DESCRIBED*	SUGGESTED CONTROL STEPS	RESPONSIBILITY
9. Extension of credit to sending bank through CHIPS or CashWire	• Credit exposure	16	• On-line net balance reporting system	DP or Operating Officer
			• Establishment of bilateral credit limit	Credit Officer/ Account Manager
			• Establishment of credit cap	Credit Officer
			• Automated controls to hold transfers that are beyond credit limit	DP or Operating Officer
10. Hardware/communications line failure	• Disruption of service	17	• Hardware, communications line back-up	DP or Operating Officer
			• Contingency off-line procedures	Operating Officer
			• Adequately trained staff	Operating Officer
			• Access to multiple funds transfer networks	Operating Officer

\*Page in this report that describes risk more fully.

109

## APPENDIX 2

# Rules of the Nationwide Task Force on Uniform Compensation

The Nationwide Task Force on Uniform Compensation (for claims arising from interbank payment errors) was formed in 1980 to develop standard compensation rules for use between the clearinghouses and other associations of financial institutions (such as the Councils on International Banking). Recognizing that local market practices dictate requirements and goals that would not apply nationally, the rules are intended for use between clearinghouses rather than within a clearinghouse or between a bank and its correspondents.

As of this printing, the Nationwide Rules have been reviewed by clearinghouses around the United States and have been adopted by many of the major clearinghouses.

## DEFINITIONS

For purposes of these rules:

"Business Days" shall be days on which the receiving party is open for business.

"Compensation" shall be a combination of penalty fees and interest computed on the amount of the principal as described in the formulas provided in these rules.

"Receiving Party" shall mean a depository financial institution that has voluntarily assented to these rules and that originally received the payment in question.

"Sending Party" shall mean a depository financial institution that has voluntarily

assented to these rules and that originally initiated the payment in question.

"Principal" is the full principal amount of the payment to be back valued.

"Fed Funds Rate" is the average of the effective Federal funds rate for the period during which the error occurred. The daily rate is published by the Federal Reserve Bank of New York.

"Number of Days" is the number of days the bank giving back valuation has lost federal availability.

"Bank" is any depository financial institution.

### Proposed Nationwide Compensation Rules

1. These rules provide procedures for settling compensation claims arising from interbank payment errors between the members of different clearing houses and associations. These rules do not replace the rules or guidelines of individual clearing houses and/or regional associations; the rules simply allow the members of one group to deal with the members of another group in an orderly fashion. They are intended to provide rules for settlement of claims between institutions with no common rule and to serve as a basis for the formulation of local or regional rules where none exists.

These rules govern compensation for lost availability and do not apply to the recovery of lost principal.

These rules are intended to provide:

- Incentive for the prompt return of funds sent in error.
- A method for the timely submission of claims.
- A method for the orderly resolution of claims.
- A general mechanism for the settling of disputes.

When an exceptional situation is encountered, it is expected that the resulting claim will be settled within the framework provided by this document, and in such a spirit that no party shall be unduly injured or enriched as the result of an error by another party.

## II. General Rules

The following general rules shall apply to all other rules presented in this document:

- A. The ultimate source, beneficiary, or type of transaction has no effect on the rules.
  - The rules apply to Federal Funds, Same-Day Funds, and Next-Day Funds between party banks.
  - The rules apply to all payments in U.S. dollars.
- B. The rules apply only to those parties agreeing to the rules, including their foreign and domestic branches.
- C. It is expected that compensation will be paid in the form of an interest check in U.S. dollars. If any other method is used, it must be agreeable to both parties. Compensation by an alternative method must have the same benefit to the parties as if the payment had been made by check.
- D. These rules do not apply to third-party errors. For the purpose of

these rules, no party to these rules shall be defined as a third party and excluded from their protection.

## III. Request for Back Valuation (Delayed Payment)

Occasionally, one party will request another party to back-value a payment the first party made for credit of an account because of a mistake on the part of the first party (the paying party).

### A. Notification

The request must express an error or omission on the part of the party requesting the adjustment and an agreement to pay proper compensation, as defined below, to the receiving party to the rules.

### B. Back Valuation

The receiving party shall make the requested back valuation after *timely* verification of the facts contained in the request, and upon receipt of correct compensation, as defined below.

### C. Back-Valuation Fee

\$100.00 must be added to any payment for back valuation. That is, after calculating the compensation amount, the party requesting the back valuation should add \$100.00 to that amount.

### D. Time Limit

Compensation will be paid for a maximum of one year. Requests for back valuation for over one year will be accommodated at the option of the party being requested to make the back valuation.

### E. Compensation

The paying party shall pay the interest amount described below or the equivalent.

The value of required compensation is based on the assumption of an overdraft in the beneficiary's account.

$$\text{Interest} = \frac{(\text{Principal}) (\text{FF Rate}) (\text{No. of days}) + 100}{360}$$

#### IV. Payment Made in Error

##### A. General Statement

When one party sends funds to another party in error, the receiving party shall return the funds as expeditiously as possible.

The receiving party has the right to contact its customer for permission to debit its account if permission is deemed necessary.

##### B. Return of Principal With Admission of Error or Indemnity

When one party pays another party in error, the receiving party shall return the funds to the sending party upon receipt of a properly authenticated request from the sending party. Such request should be in the form of an authorized message requesting the receiving bank to debit the account originally credited in error and return the funds to the paying party. The receiving party has the right to contact the customer to be debited for permission to debit the account, if such permission is deemed necessary.

There are two types of the properly authenticated request which expedite the return of funds sent in error by parties to the rules. The first contains an admission that the error was made by the sending party. The second contains an indemnification issued to the receiving party by the sending party.

The receiving party will compensate the payment party for the value of the funds while they were on deposit at the receiving party.

If the funds are returned to the sending party within 5 business days of the receipt of the request or indemnification, \$500.00 may be deducted from the compensation.

Any time of day is defined as the receipt day. The idea is to give four full business days to return the item. Therefore, the time of receipt on the first day is immaterial.

This time-limit applies only to the return of the principal requested by one of these two types of requests. The receiving party does not have to honor either type of request for the time limit to apply.

If the party that received the funds in error fails to return the principal within the time limit, it may not deduct the \$500.00 from the compensation amount; however, it may deduct \$100.00 from the compensation amount. It should be understood that delays due to seeking debit authorization are not grounds for an extension of the time limit.

##### C. Compensation

The receiving party shall pay to the sending party the amount of interest described below or the equivalent.

$$\text{Interest} = \frac{(\text{Prin.}) (1 - \text{Res. Req.}) (\text{FF Rate}) (\text{No. Days})}{360} \quad \text{(see below)}$$

1. For return of principal within 5 business days, deduct \$500.00 from the interest amount.
2. For return of principal under indemnity or with an admission of error by the sending party in more than 5 business days,

deduct \$100.00 from the interest amount.

3. The receiving party may deduct \$500.00 from the interest amount in other cases when there is no indemnity or when admission of error is involved.

For instance, if the receiving party recognizes the payment in error and returns the principal prior to receiving a request, it may deduct \$500.00 from the interest amount.

If the receiving party is paid early and is asked to adjust the value and pay compensation for entitlement, it may deduct \$500.00 from the interest amount.

If the paying party requests the return of principal paid in error but does not use an indemnity or admission of its own error, no limit will apply and \$500.00 may be deducted from the interest amount.

For return of principal prior to request or without indemnity or for early payment, deduct \$500.00 from the interest amount.

#### D. Time Limits

1. Claims for compensation must be initiated within 90 calendar days following the return of the funds.
2. The maximum amount of compensation to be paid is the last 180 calendar days of the error period.

#### V. Change of Beneficiary

On occasion, the sending party makes a payment to the wrong receiving party or to a credit to the wrong account, or omits the account name.

The receiving party will, upon receipt of notification, adjust the beneficiary of the payment on its books. If the receiving party had use of the funds during the period of the error, it will adjust the value date of the transaction to the original transaction date upon receipt of proper compensation as defined.

#### A. Notification

When requesting an adjustment of beneficiary, the sending party will provide the receiving party with a satisfactory authenticated request or indemnity which may be in the form of an authorized message to the receiving party. The message shall request the receiving party to debit its account originally credited in error. The receiving party has the right to contact the customer for permission to debit its account, if such permission is deemed necessary. The sending party shall also indicate agreement to pay proper compensation, as defined below, to the receiving party.

#### B. Amendment of Beneficiary Fee

\$100.00 will be charged for request to amend beneficiary.

\$100.00 fee will be paid regardless of whether back valuation is required.

For beneficiary changes requested between two foreign branches of the receiving party, there is no reserve loss, and no compensation is required, but the \$100.00 fee applies.

The compensation period for the change of beneficiary will end on the fourth business day following notification by wire from the sending bank of the error. An indemnity is optional and the receiving member party does not have to accept the indemnity for the limit to apply. Any time of day is defined as the

receipt day. The idea is to give four full business days to amend the item; therefore the time of receipt on the first day is immaterial.

### C. Compensation

The receiving party shall be compensated for assumed losses incurred due to excess reserves maintained as a result of overdrafts on the account of the correct beneficiary during the period the incorrect account was credited. Compensation shall be paid as interest in the amount defined below.

The compensation period will end on the 4th business day following receipt of the authorized message.

Any time of day is defined as the receipt day. The idea is to give four full business days to adjust the beneficiary. Therefore, the time of receipt on the first day is immaterial.

$$\text{Interest} = \frac{(\text{Prin.}) (\text{Res. Req.}) (\text{FF Rate}) (\text{No. Days})}{360} + \$100.00$$

### D. Time Limits

In the absence of mutual agreement, the receiving party is not required to apply the credit to the correct customer's account with more than 180 calendar days of back value. In turn, the sending party is required to compensate the receiving party only for the period covered by the back valuation. This time-limit recognizes that the receiving party may be limited to the most recent 180 calendar days in its ability to ensure that it had use of the funds in the incorrect customer's account.

Further, the receiving party is not required to adjust the value more than 180 calendar days prior to the request for the amendment of beneficiary.

## VI. Bank-to-Bank Drawdown Request

### A. Failure to Respond

When a party fails to respond to a timely drawdown request, the party making the error shall compensate the other bank for the period that the funds were not sent, as if it were a late payment.

There is a fee of \$100.00.

$$\text{Interest} = \frac{(\text{Principal}) (\text{Average Fed Funds}) (\text{Number of Days})}{360} + \$100$$

### B. Time Limits

Claims for compensation must be initiated within 90 calendar days following the error.

## VII. Other Compensation Claims

For compensation claims for errors or delays not specifically addressed, it is expected that parties to these rules will cooperate in settling such claims.

## SAMPLES OF GUARANTEE (OPTIONAL)

### Funds Transfers Made in Error

ATTN: \_\_\_\_\_ RE OUR \_\_\_\_\_ DATED  
\_\_\_\_\_ FOR \$\_\_\_\_\_ IN FAVOR OF \_\_\_\_\_  
BY ORDER OF \_\_\_\_\_. AS THE ABOVE  
PAYMENT WAS NOT INTENDED FOR YOUR-  
SELVES, KINDLY REFUND THE AMOUNT  
\$\_\_\_\_\_. BECAUSE OF AN ERROR ON OUR  
PART AND IN CONSIDERATION OF YOUR  
ACTING ON THIS REQUEST, WE HEREBY  
AGREE TO HOLD YOU FREE AND HARMLESS  
AGAINST ANY AND ALL CLAIMS, LIA-  
BILITIES, LOSSES, SUITS, OR DAMAGES  
WHATSOEVER ARISING THEREFROM,  
INCLUDING COSTS AND EXPENSES. WE  
FURTHER AGREE TO REFUND THE AMOUNT  
RETURNED UPON DEMAND. KINDLY CON-  
TACT YOUR CUSTOMER FOR  
CONFIRMATION OF YOUR ACTIONS TO  
RELEASE US FROM OUR INDEMNITY.

LEGEND

1-PERFORMANCE INDICATORS

The three most commonly used type of performance indicators are:

1. Volume - quantity measures that indicate performance of tasks (e.g. deposits).
2. Efficiency - indicators that divide a measure of output by a measure of input (e.g. deposits processed per hours worked).
3. Exception - indicators that report information that normally reflect errors or problems (e.g. number of box outs in the vault).

2-EXPOSURE/MEDIAN

The assessed level of exposure in dollars for the major activity prior to the placement of any controls.

Low - \$0 to \$100,000

Medium - \$100,000 to \$1,000,000

High - \$1,000,000 and over

3-EXISTING CONTROLS

P = Preventative Control: A control that is in place to reduce the probability of an error occurring.

D = Detective Control: A control that is in place to determine whether an error has occurred.

4-PROBABILITY OF LOSS

The approximate frequency of occurrence.

Low - once a year

Medium - once a month

High - once a week

5-EXPOSURE

The assessed level of exposure in dollars for the major activity with existing controls in place.

6-PROPOSED CONTROLS

The estimated level of exposure in dollars for the major activity once the proposed controls have been implemented.

L = Low - \$0 up to \$100,000

M = Medium - \$100,000 up to \$1,000,000

H = High - \$1,000,000 and over

RISK ASSESSMENT SURVEY  
OVERVIEW  
Page 1

	MAJOR ACTIVITY	ENVIRONMENT AFFECTED	POSSIBLE CAUSE OF EXPOSURE	PERFORMANCE INDICATORS	EXPOSURE/MEDIAN (N/M/L) DOLLARS	EXISTING CONTROLS	CONTROL EFFECTIVENESS	PROBABILITY OF LOSS (N/M/L)	EXPOSURE (N/M/L)	PROPOSED CONTROLS
1	Non-Automated Processing	All Operations Areas	Greater production volumes may cause increased errors and backlog of work.	Weekly Dept. Management Report Monthly Management Report Aged Open Items Reports	Low	Review of operational efficiency needs by <u>Operational Planning/Risk Management</u> . (P)  Current management report (P)  All operational areas and volumes using statistics gathering methodology and business forecasting techniques currently in pilot phase. (P)	Effective	Low	Low	Implement project prioritization list with cost justifications, assigned responsibilities and weekly status updates. (L)  Develop a greater in-depth management report. (L)  Continued review of operating areas by <u>Operational Planning/Risk Management</u> . (L)
2	Operations Procedures Writing	All Departments	Procedure changes over time to where normal controls no longer	<u>Internal Audit Report</u>	Low	Annual review of departmental procedures	Effective	Low	Low	Procedure prioritization

BEST AVAILABLE COPY

1/19

MAJOR ACTIVITY	ENVIRONMENT AFFECTED	POSSIBLE CAUSE OF EXPOSURE	PERFORMANCE INDICATORS	EXPOSURE/MEDIAN (N/P/L) DOLLARS	EXISTING CONTROLS	CONTROL EFFECTIVENESS	PROBABILITY OF LOSS (N/P/L)	EXPOSURE (N/P/L)	PROPOSED CONTROLS
4 New System Turnover	<i>REPOSITORY PARTICIPANTS</i>	Customer leaving due to erroneous processing when sufficient program string and stress tests were not done.	<u>Stress Test Results</u> <u>System Functionality Test Results</u> <u>24-Hour Test Results</u> <u>Multiple Day Test Results (parallel testing)</u>	High	Review by Systems Analyst, Product Analyst and Operations Manager with appropriate sign-offs on various test results. (P)	Adequate	Low	High	
5 Mark-to-Market Value Positions		Firm goes under and cannot cover settlement debit owed to MSTC which includes mark-to-market.	Surveillance Update Sheet	High	Surveillance monitors reports daily and receives information on firms in possible trouble. These are placed on a "watch" list. In the event firm does cease to exist, able to unwind trades prior to comparison. Loss would be restricted to the mark-to-market which is covered by Participant Fund. (P)	Effective	Low	Low	Creation of report indicating large mark-to-market for individual securities prior to settlement. (L)
		Price is bad on stock causing large settlement debit which firm cannot pay.	Surveillance Mark-to-Market Report Firm Activity Reports	Low		Effective	Low	Low	
6 Miscellaneous Billing	Participants All <i>DEP</i> Operating Depts Accounting Participant Services Marketing	Manual procedure allows errors where firms are not charged or over charged for services.	Operations Log or Tally Sheets	Low	Dually prepared adding machine tapes. (P)  Control Report totals are used for miscellaneous billing. (P)	Adequate	Low	Low	Automation of all billing charges and better breakdown of charges. (L)
		format codes not picked up on automated billing.		Low		Adequate	Low	Low	
		Inadequate breakdown of billing charges. Charges reversed when challenged.		Low		Adequate	Low	Low	

REST AVAILABLE COPY

*SAMPLE*

X

MAJOR ACTIVITY	ENVIRONMENT AFFECTED	POSSIBLE CAUSE OF EXPOSURE	PERFORMANCE INDICATORS	EXPOSURE/MEDIAN (N/M/L) DOLLARS	EXISTING CONTROLS	CONTROL EFFECTIVENESS	PROBABILITY OF LOSS (N/M/L)	EXPOSURE (N/M/L)	PROPOSED CONTROLS
		Violation of SEC Rule 15c2-3 where all parties to a trade do not have all the same information available.		Low		Adequate	Low	Low	
10	Bearer Bonds Custodial Processing	Depository Satellite Custodian	Rules of contract governing processing are too broad.	Aged Open Transit	High	Aged Open Transit Exceptions Report review by Management (P)	Effective	Low	Low
			Unaware of exact processing procedures and/or controls.	Exception Report	High		Effective	Low	Low
11	Participants Agreement	DEPOSITORY Participants	Participant initiates activity before agreement is signed and approved.	Activity Report	Low	SEC-15c2-3, Federal Reserve Regulation, and other applicable regulations.	Effective	Low	Low
			Participant liquidates before closing all positions and settling charges.	Participant Report	Low	SEC-15c2-3, Federal Reserve Regulation, and other applicable regulations.	Effective	Low	Low
12	Training of Employees	DEPOSITORY Participants	Lack of sufficient training and improper procedures documentation increases the chances of employee errors.	Performance Reviews	High	Informal department training. (P)	Inadequate	High	High
			Not enough segregation of duties by employees.	Performance Reviews	High		Inadequate	High	High
13	Employee Vacations	Inter-Department	Fraud schemes undertaken when there is no cross-training of duties.	Decrease in income and cash.	Low	Bonding of employees limits exposure. (P)	Inadequate	Low	Low

BEST AVAILABLE COPY

X  
 SAMPLE

MAJOR ACTIVITY	ENVIRONMENT AFFECTED	POSSIBLE CAUSE OF EXPOSURE	PERFORMANCE INDICATORS	EXPOSURE/MEDIUM (R/P/L) DOLLARS	EXISTING CONTROLS	CONTROLS EFFECTIVENESS	PROBABILITY OF LOSS (R/P/L)	EXPOSURE (R/P/L)	PROPOSED CONTROLS	
14	Hiring of Personnel	Inter-Department	Too many semi-permanent employees in secured areas that do not have any responsibility to <b>NECESSITARY</b>	Medium	None	Inadequate	Low	Medium	Hire permanent employees when possible. (L)	
15	Screening of Employees	Inter-Department	Employees are not screened or screened only periodically.	Medium	Security Check Reports	Program established to re-fingerprint employees with over five years tenure. (D)	Adequate	Low	Medium	Fingerprint on day hired and not on day new employee starts. (L)  Keep new employee under constant review until FBI report is received. (L)
16	Corporate Travel	Inter-Department	Key employees traveling in same vehicle that crashes resulting in death of employees.	Low	None	Inadequate	Low	Low	Establishment of a Corporate Travel Policy. (L)	
17	Receipt of Securities Through Mail	Mailroom All Internal Departments	Securities sent to corporate address and are directed to the Mailroom. The room is unlocked and opens to a public access area. Possibility exists for lost securities.	Medium	Lost Certificate Report	Firms have standing instruction to send securities to P.O. Box or to drop off items at Distribution window. (P)	Inadequate	Medium	Medium	Put Mailroom under secured environment. (L)
			Securities delivered to departments in non-secured areas.	Medium				Inadequate	Medium	Medium

BEST AVAILABLE COPY

X  
SAMPLE

119

	MAJOR ACTIVITY	ENVIRONMENT AFFECTED	POSSIBLE CAUSE OF EXPOSURE	PERFORMANCE INDICATORS	EXPOSURE RISK/ (L/N/Y)/ CLASS	CONTROL MEASURES	POSSIBILITY OF LOSS (N/Y/L)	EXPOSURE (L/N/Y/L)	PROPOSED CONTROLS
22	All Operational Processing	<i>DEPOSITORY</i> Participants	Disaster renders operations areas unusable.	Life-safety monitoring systems feedback.	High	Life-safety monitoring systems. (P)	Adequate	Low	Contingency plan to restore operations at alternate location. (L)

*SAMPLE*

X

BEST AVAILABLE COPY

*MP*

RISK ASSESSMENT SURVEY  
INTERFACE POSITION BALANCE

MAJOR ACTIVITY	ENVIRONMENT AFFECTED	POSSIBLE CAUSE OF EXPOSURE	PERFORMANCE INDICATORS	EXPOSURE (N/P/L)	CONTROL	CONTROL EFFECTIVENESS	POSSIBILITY OF REPEAT (N/P/L)	EXPOSURE (N/P/L)	PROPOSED CONTROLS
1 Identification of Position Out-of-Balance Between Interfaces	Interface Participants Inter-Department	Improper identification	Break Report	Low	Notification of Breaks to assigned departments. (P)	Effective	Low	Low	
		Missing reports	Weekly/Monthly Management Reports	Low		Effective	Low	Low	
		Offsetting breaks cancelling	Audit Packages	Low	Changes on break report of amount or date are identified via the program. (P)	Effective	Low	Low	
		Short value position not reflected on break report		Low		Effective	Low	Low	Add to existing program the ability to identify short position on break report. (L)
2 Adjustment of Interface Related Breaks	Interface Participants	Wrong adjustment made	Break Report	Low	Increased numbers on "Aged Out of Balance" report to management. (D)	Effective	Low	Low	Break tracked on P.C. for better tracking and follow-up. (L)
		Adjustment not processed	Participant or Inquiries	Low		Effective	Low	Low	
3 Processing Incoming/Outgoing Deliveries (inventory movements for free)	Participants	Delivery not processed	Activity Reports	Low	Daily review of manual break reports and assignment to proper departments for resolution. (D)	Effective	Low	Low	
		Delivery not processed correctly		Low		Effective	Low	Low	

BEST AVAILABLE COPY

SAMPLE

X

RISK ASSESSMENT SURVEY  
MANDATORY DEPT.

Page 1

MAJOR ACTIVITY	ENVIRONMENT AFFECTED	POSSIBLE CAUSE OF EXPOSURE	PERFORMANCE INDICATORS	EXPOSURE/FREQUENCY (N/A/L) DOLLARS	EXISTING CONTROLS	CONTROL EFFECTIVENESS	PROBABILITY OF LOSS (H/M/L)	EXPOSURE (N/A/L)	PROPOSED CONTROLS
1 Notification of Offer	REPOSITORY Participant	Erroneous information	Second notice by agent/company	Low	Duplicate information sources (P)	Effective	Low	Low	
		Notification source not received.	Participant Inquiry						
		Security/offer misidentified.							
		Clerk does not act on information. Does not prepare file.							
		Security is not frozen.	Freeze Update Screen	Low	Rep review (P)	Effective	Low	Low	
2 Offer Assignment	REPOSITORY Participant	Offer is not assigned.	Offer file Participant Inquiry	Low	Duplicate information source (P)	Effective	Low	Low	
3 Participant Notification	REPOSITORY Participant	REORG reorganization notice is not released to participants, or has incomplete or inaccurate information reported.	REORG Reorganization Notice Participant Inquiry	Low	Supervisor review (P)	Effective	Low	Low	
		Failure to allow firms their dissenter rights on relevant offers by not making information and shares available to them.	Offer Statement Participant Inquiry	Low	Supervisor awareness of dissenters rights made known by reading "OS" when assigning offer. (P)	Effective	Low	Low	
4 Inventory Control	REPOSITORY Participant	Securities not available for shipment to agent due to position differences with TRFS, vault, offsites.	Aged Transfer Report Tracking Report Box Out Report Break Report	Low	Balancing reverification (D) Resolution of box outs, breaks, TRFS, offsites. (D)	Adequate	Low	Low	

BEST AVAILABLE COPY

SAMPLE

X

MAJOR ACTIVITY	ENVIRONMENT AFFECTED	POSSIBLE CAUSE OF EXPOSURE	PERFORMANCE INDICATORS	EXPOSURE/MEDIAN (N/M/L) DOLLARS	EXISTING CONTROLS	CONTROL EFFECTIVENESS	PROBABILITY OF LOSS (R/M/L)	EXPOSURE (N/M/L)	PROPOSED CONTROLS
1 Notification of Bearer System Call Information by Custodian	Custodian Participants <i>DEPOSITORY</i>	Source does not notify or notifies incorrectly.	Custodian notifies Muni operations.	High	Tracking system for notifications received. (P)	Effective	Low	Low	
		Notification information received by Midwest but not by Muni Operations.		High	Automated input of notifications into the Call Bond System. (P)  exposure limited on claims arising from custodian errors. (P)  Duplicate call notification sources. (P)	Effective  Effective	Low  Low	Low  Low	
2 Search Process for Called Securities	<i>DEPOSITORY</i> Participant Custodian	Erroneous information.	Notice by paying agent.	LOW	Shortage research in Interest Dept. (D)	Adequate	LOW	LOW	
		Misread information causing incorrect amount of securities to be processed.	Missed Interest Pay Report  Depository Interface Break Report	LOW	Loss limited to one coupon payment when custodian is responsible for missed call. (D)	Adequate	LOW	Low	

BEST AVAILABLE COPY

*SAMPLE*

BEST AVAILABLE COPY

X

RISK ASSESSMENT SURVEY  
 SETTLEMENT AND COLLECTION BANKING  
 PAGE 1

*low  
Set.*

MAJOR ACTIVITY	ENVIRONMENT AFFECTED	POSSIBLE CAUSE OF EXPOSURE	PERFORMANCE INDICATORS	EXPOSURE/MEDIAN (N/M/L) DOLLARS	EXISTING CONTROLS	CONTROL EFFECTIVENESS	PROBABILITY OF LOSS N/M/L	EXPOSURE (N/M/L)	PROPOSED CONTROLS
1 Sending Wire Transfers	<i>DEPOSITORY</i> Participants Federal Reserve Settlement Collection Banking Other Depositories Other Clearing Corps.	Improper wire due to: - clerical error - fraud	Bank Balance Statements  Bank Reports  Fed Wire Statements	High	Verification of Bank Statements and daily reports through the daily balancing functions and shortage research. (D)	Effective	Low	Low	
		All payments with Fed funds		High	- All wire transfers are confirmed by clerk other than preparer. (P) - All wire transfers are verified by a second clerk. (P)	Effective	Low	Low	
		Wires are immediate and final		High	Supervisor provides additional code for Fed wire transfer or ensure proper authorization. (P)	Effective	Low	Low	
2 Physical Check Disbursement	<i>DEPOSITORY</i> Participants Settlement Collection Banking Non-Members Other Depositories Other Clearing Corps.	Overpayment to participants/claimants.	Bank Balance Statements  Collection Banking Cash Balance Report	Low	Verification of Bank Statement and daily reports through the daily balancing functions. (D)	Effective	Low	Low	
		Individuals make check payable to themselves.	Over/Short Reconciliations  Daily Bank Reports	Medium	- Division of duties within dept. Person issuing check doesn't reconcile accounts. (P) - Supervisor reviews all cancelled checks to ensure payee was not altered. (D)	Effective	Low	Low	

BEST AVAILABLE COPY

*Attended  
Dpt. - 800211.  
Bank*

*X  
SAMPLE*

*1/24*

RISK ASSESSMENT  
UNDERWRITING

MAJOR ACTIVITY	ENVIRONMENT AFFECTED	POSSIBLE CAUSE OF EXPOSURE	PERFORMANCE INDICATORS	EXPOSURE/MEDIAN (R/M/L) DOLLARS	EXISTING CONTROLS	CONTROL EFFECTIVENESS	PROBABILITY OF LOSS (H/M/L)	EXPOSURE (H/M/L)	PROPOSED CONTROLS
1 Processing and Underwriting	Participant Inter-department <i>DEPOSITORY</i> Issuer of New Security Bond Council	Participant Involved as syndicate manager has financial problems	Surveillance Dept. Watchlist	Low	Comparison of underwriting report to surveillance daily watchlist. (D)	Adequate	Low	Low	
		<i>DEPOSITORY</i> agrees to make eligible but fails to do so (participants claim for any loss)	Terminal Inquiry Screen	Low	<i>DEPOSITORY</i> continuously monitors	Adequate	Low	Low	
		Loss of certificates internally once received from issuer for safekeeping	Security and Box Out Reports Tracking Report	Low	Good delivery check performed by Security Receipts. Certificates counted and matched to registration. (P)	Effective	Low	Low	Establish a release code with the issuer for each underwriting. (L)
		Human error by syndicate manager or personnel resulting in improper notification of close	Syndicate Member Notification	Low	Participant update verified by two independent people before update is processed. Proper I.D. is required. (P)	Adequate	Low	Low	
		<i>DEPOSITORY</i> updates wrong broker	Activity Reports	Low					
		System delays or downtime	Computer "Flash" Report	Low					

BEST AVAILABLE COPY

BEST AVAILABLE COPY

X  
SAMPLE

103

RISK ASSESSMENT SURVEY  
DATA SECURITY

MAJOR ACTIVITY	ENVIRONMENT AFFECTED	POSSIBLE CAUSE OF EXPOSURE	PERFORMANCE INDICATORS	EXPOSURE/MEDIAN (N/M/L) DOLLARS	EXISTING CONTROLS	CONTROL EFFECTIVENESS	PROBABILITY OF LOSS N/M/L	EXPOSURE (N/M/L)	PROPOSED CONTROLS
1 Issue I.D.'s, Passwords	All	Inappropriate - issued to wrong person.	Security Access Reports	Medium	Forms containing request for I.D.'s and passwords are authorized by firm and Vice Presidents internally. (P) - All authorizations are maintained in a locked file. (P) - Audit trail reports reviewed weekly for unauthorized access. (D)	Adequate	Low	Low	Passwords to be changed every 30 days to prevent sharing. (L)
		Improperly distributed - issued to non-employee.	Audit Trail Reports	Medium		Adequate	Low	Low	
		Invasion of privacy - password information leaked.		Medium		Adequate	Low	Low	
2 Allow Access to Data	All	Unlimited access - authorization too global.	Security System Reports Audit Trail Reports	Medium	Same forms used in above also contain program/data authorizations for individuals. Data Security Analyst reviews all conflicting items with departments involved. (P)  Audit trail reports reviewed weekly for unauthorized access. (D)	Adequate	Low	Low	Passwords to be changed every 30 days to prevent unauthorized access to data. (L)
		Inappropriate - issued to wrong person.	On-Line Simulation of Access	Medium		Adequate	Low	Low	
3 Monitor All Security Violations	All	Untimely - not detecting violations promptly after occurrence.	Exception Reports from Top Secret	Medium	Review by Data Security Analyst of exception reports on weekly basis and follow-up with users where appropriate. (P) - Real-time on-line monitoring/ notification (D)	Adequate	Low	Low	

BEST AVAILABLE COPY

BEST AVAILABLE COPY

X  
SAMPLE

1/26

MAJOR ACTIVITY	ENVIRONMENT AFFECTED	POSSIBLE CAUSE OF EXPOSURE	PERFORMANCE INDICATORS	EXPOSURE/MEDIAN (N/M/L) DOLLARS	EXISTING CONTROLS	CONTROL EFFECTIVENESS	PROBABILITY OF LOSS (N/M/L)	EXPOSURE (N/M/L)	PROPOSED CONTROLS
1 Batching Hardcopy Input	All	Improper dissemination of batches by the batch clerk. Batch can be overlooked.	<u>Participant</u> <u>Communique</u>	Medium	Data Control does: - a batch test against batches keyed to identify batches not yet submitted. (D)  Manual review by Data Control at cut-time of batches input against batches received which are listed on Batch Control Log. (D)	Adequate	Medium	Medium	
		Duplicate batches entering system. Input is heavy before input close and last pass close. Due to heavy input, valid information does not get keyed. Emphasis on getting batches to operators at those times.		Low	Batch clerk reviews all batches to catch duplicate batch numbers. (P)	Adequate	Medium	Medium	

X

SAMPLE

BEST AVAILABLE COPY

187

MAJOR ACTIVITY	ENVIRONMENT AFFECTED	POSSIBLE CAUSE OF EXPOSURE	PERFORMANCE INDICATORS	EXPOSURE/MEDIAN (N/N/L) DOLLAR	EXISTING CONTROLS	CONTROL EFFECTIVENESS	PROBABILITY OF LOSS N/N/L	EXPOSURE (N/N/L)	PROPOSED CONTROLS
2 Data Entry	Participants Data Entry	Improper keying techniques.	Verification Reports	Low	Operators re-key batches to verify all input each day before information is released into the main frame applications. (D)  - System edits money on batch against individual money on each ticket in the batch to balance. (D)	Effective	Low	Low	Retrieve on-line deposit tickets and compare with original deposit ticket. (L)
		Choosing wrong program level for data entry.	<i>VERIFICATION REPORTS</i>	Low	- System edits number currip and does a preliminary edit for data. Operations Dept. notified of reject. (D) - Operators rekey batches to verify all input each day and cancel all tickets on batches input at the end of the day. (D)	Effective	Low	Low	
		Improper value input for on-line real-time bearer system resulting in settlement debit that participant is unable to pay.	<del>Bearer System Audit Trail Report for Input</del>	Low	Sight verification by input operator. (P)  Operator initials ticket. (D)	Inadequate	Medium	Low	
3 Disk to Tape Processing	Participants Data Entry	Incorrect execution of procedures (incorrect autoprompts, wrong job I.D.'s for entry into the system) can cause bad tapes. Time pressures exist. Recovery time is dependent upon when it happened and when it was discovered.		Medium	Main frame operator notifies Data Entry Tape Writer that input was rejected for incorrect blocking factor. Tape is recreated by the tape writer and then verified. It is then verified again before tape is created. (P)	Effective	Low	Medium	

BEST AVAILABLE COPY

*SAMPLEX*

*1/78*

MAJOR ACTIVITY	ENVIRONMENT AFFECTED	POSSIBLE CAUSE OF EXPOSURE	PERFORMANCE INDICATORS	EXPOSURE/MEDIAN (N/H/L) DOLLARS	EXISTING CONTROLS	CONTROL EFFECTIVENESS	PROBABILITY OF LOSS N/H/L	EXPOSURE (N/H/L)	PROPOSED CONTROLS
1 Processing of Data for	<i>DEPOSITORY</i> Participants Other Clearing Corps Other Depositories	Hardware outages	Error messages from operating system Error messages from helon panel Error messages from site master	High	Hardware Device Status Reports reviewed daily by IBM service engineers. (P) - Maintenance agreement with IBM provides 7-day, 24-hour coverage. (P)	Effective	Low	High	Hot site off premises for data processing. (H)
		Power outages	Hourly security walk through	High	Two separate power feeds from two different power stations feed computer floor. (P) - An uninterrupted power supply is in place to provide 15 minutes of power in the event of an outage and to ensure an orderly shutdown. (P)	Effective	Low	High	
		Fire		High	Helon and sprinkler systems exists. (P) - Plastic sheeting to protect computer from water damage. (P)	Effective	Low	High	
		Flood		High	Curbing exists in the perimeter of computer floor to prevent flooding. Curbing is membrane treated and alarms are in place. (P)	Effective	Low	High	
		Disaster destroying entire data center		High	File backups are stored offsite daily for all major applications and operating systems. (P)	Effective	Low	High	
2 Transmission of Data	<i>DEPOSITORY</i> Participants Other Clearing Corps Other Trust Companies	Fire	Monitoring equipment that identifies line failure, dropped lines, and equipment failure.	Low	On-line monitoring of circuits and equipment. (D)	Adequate	Low	Low	Hot site off premises with alternate telephone master station. (L)
		Loss of telephone company circuits		Low	Backup circuit between Chicago and New York. (P)	Adequate	Low	Low	Dial-up backup offered as alternative to leased lines. (L)

X  
SAMPLE

1/28/80

MAJOR ACTIVITY	ENVIRONMENT AFFECTED	POSSIBLE CAUSE OF EXPOSURE	PERFORMANCE INDICATORS	EXPOSURE/MEDIAN (N/N/L) DOLLARS	EXISTING CONTROLS	CONTROL EFFECTIVENESS	PROBABILITY OF LOSS N/N/L	EXPOSURE (N/N/L)	PROPOSED CONTROLS
		Loss CPU Power Loss Equipment Failure			Backup network controller. (P)	Adequate	Low	Low	
3	Software Modification <i>DEPOSITORY</i> Participants Other Clearing Corps. Other Trust Companies	Erroneous changes to software	Application availability	High	Formal change control document signed by manager. (D) Formal plan to test changes. (P) Contingency backout plan. (P)	Adequate	Low	Low	Parallel production processing system to ensure new software performs to specifications. (L) System stress tests. (L) Purchase of additional monitoring and debugging software. (L)
4	Creating and Modifying Definitions of Production Databases <i>DEPOSITORY</i> Participants Other Clearing Corps. Other Trust Companies	Inaccurate or missing data	Database availability percentage	Medium	Thorough testing prior to implementation. (P) Controlled post implementation testing. (D) Ongoing monitoring of performance data. (D) Periodic integrity audit programs. (P)	Adequate	Low	Low	
5	Modify and Update Database System Software <i>DEPOSITORY</i> Participants Other Clearing Corps. Other Trust Companies	Database system outage.	Database availability percentage	Medium	Thorough testing prior to implementation. (P) Controlled post implementation testing. (D)	Adequate	Low	Low	
		Performance degradation.		Medium	Ongoing monitoring of performance data. (D) Periodic integrity audit programs. (P)	Adequate	Low	Low	

BEST AVAILABLE COPY

X

SAMPLE

RISK ASSESSMENT SURVEY  
PARTICIPANT SERVICES

MAJOR ACTIVITY	ENVIRONMENT AFFECTED	POSSIBLE CAUSE OF EXPOSURE	PERFORMANCE INDICATORS	EXPOSURE/MEDIAN (N/P/L) DOLLARS	EXISTING CONTROLS	CONTROL EFFECTIVENESS	PROBABILITY OF LOSS N/P/L	EXPOSURE (N/P/L)	PROPOSED CONTROLS
1 Data Entry on Behalf of Participant by Participant Services	Participant <i>DEPOSITORY</i> Participant Services Surveillance	Input error causes value error. Participant doesn't pay and loses the interest.	Unpaid Debit Report	Low	Participant Services Representative act at the direction of participants. Hardcopy is provided to participants for review. We act as agent for firm and accept no liability for errors. (D)  Supervisor signs off on all position adjustments. (D)	Adequate	Low	Low	Copy of Documentation forwarded to Surveillance for consideration in determining recovery of interest. (L)
2 Cash Adjustments and Manual Adjustments	Participant <i>DEPOSITORY</i> Participant Services	Collusion between Participant Services Rep and participant's personnel	Monthly Participant Audit Reports	Low	Supervisor signature is needed on all cash adjustments under \$250,000. Manager's signature is needed on amounts above that. (P)	Effective	Low	Low	Automate cash adjustments using terminal. (L)
		Clerk error.	Activity Report	Low		Effective	Low	Low	
3 Mark-to-Market Adjustment on Member-to-Member Stock Loans	Participants <i>DEPOSITORY</i> Participant Services	Participant effects loan, provides service, the money moves for the wrong amount.	Participant Communication	Low	<del>Participant Services</del> Participant Services acts as agent and accepts no liability for errors. (P)	Effective	Low	Low	Automate marks on terminal between participants. (L)

*SAMPLE*

*Participant Services  
Supervisor  
Manager  
Hardcopy  
Documentation  
Surveillance  
Recovery  
Interest  
L*

X

131

**APPENDIX C**

**TRAINING MATERIALS ON COMPLIANCE,  
SURVEILLANCE, AND RISK MANAGEMENT**

**INTRODUCTION TO  
COMPLIANCE, SURVEILLANCE, AND RISK MANAGEMENT  
AS RELATED TO A SECURITIES DEPOSITORY**

**Presented to National Securities Depository Limited of India (NSDL) By:**

**Sue Hertel  
Consultant  
Price Waterhouse**

## BACKGROUND

Under the organizational development of the depository, NSDL has designated departments of Compliance, Surveillance, and Risk Management. The management of these areas requested that Price Waterhouse provide ideas on specific responsibilities for each area. The following outlines are offered in response to those requests.

In addition, copies of several topic-related publications are being provided to NSDL. It is intended that this information will provide NSDL with insight on how other organizations have addressed these issues and recommendations given by some of the U.S. regulators.

Finally, a sample chart for use in the analysis of risk within the depository is also provided. Use of such a chart by NSDL will help to organize the thought process in identifying areas of risk to be monitored and controlled. Similar charts may also be developed in the areas of compliance and surveillance.

Once specific potential areas of compliance, surveillance, and risk management are identified, NSDL should develop internal operating policies and procedures related to these areas. Price Waterhouse is prepared to assist in the development of both the analysis charts and the internal procedures. NSDL will then need to make policy decisions in certain areas of risk and surveillance.

The information and suggestions being provided here and any resultant procedures are only a beginning. NSDL should submit the charts and procedures to their internal and external legal counsel as well as regulators for review, comment, and/or approval.

The analyses and procedures must then be reviewed by NSDL on an ongoing basis (at minimum, annually) to insure all areas of exposure, risk, and compliance continue to be addressed by the depository. In addition, NSDL's internal and external auditors should include reviews in these areas in audit plans. It is also expected that industry regulators will regularly evaluate such policies and procedures.

## OBJECTIVES

**COMPLIANCE OBJECTIVE:**

To insure that the depository complies with all industry regulations, corporate business rules and bye-laws.

**SURVEILLANCE OBJECTIVE:**

To protect the depository, its participants, and the beneficial owners of securities held at the depository against financial and operational failure by a depository participant.

**RISK MANAGEMENT OBJECTIVE:**

To limit risk to the depository corporation that results from depository services provided to participants as well as internal corporate activity.

135

## COMPLIANCE ISSUES FOR NSDL

OBJECTIVE: To insure that the depository complies with all industry regulations, corporate business rules and bye-laws.

### APPROACH:

- \* Identify all facets of compliance to monitor based on industry regulations, corporate business rules, and bye-laws.
- \* Review changes in industry regulations for impact on depository processing.
- \* Develop techniques for monitoring depository processing and policies to insure compliance with regulations.
- \* Review/approve documented depository procedures for compliance to regulations.
- \* Review/approve new products developed and changes made to existing products.
- \* Recommend actions to be taken on non-compliance situations.
- \* Work with regulators on depository and industry issues.

## SURVEILLANCE ISSUES FOR NSDL

OBJECTIVE: To protect the depository, its participants, and the beneficial owners of securities held at the depository against financial and operational failure by a depository participant.

### APPROACH:

- \* Review applicants for financial and operational soundness, insuring NSDL standards are met.
- \* Periodic review of financial reports on participants.
- \* Annual examination of participants' facilities, books and records.
- \* Ongoing monitoring for/of unusual activity in a participant's account.
  - Concentration in one security
  - Pledge of securities
  - Proper segregation/recording of customer securities
- \* Sharing of information on common participants with exchanges, clearing corporations, and other depositories.
- \* Work with regulators on participant issues and beneficial holdings.
- \* Monitor newspapers and trade publications for indicators of financial or operational problems at a participant.
- \* Immediate action to protect depository positions as necessary.
- \* Requirement of participant fund deposits in excess of standard amount as necessary to limit risk.
- \* Recommendations on actions to be taken against participants creating risk to the depository system.
- \* Application of any penalties against participants

\* Preparation of internal watch lists and reports on surveillance issues.

## RISK MANAGEMENT ISSUES FOR NSDL

OBJECTIVE: To limit risk to the depository corporation that results from depository services provided to participants as well as internal corporate activity.

### APPROACH:

- \* Identification of areas of risk.
  - Operational procedures, policies, and processes
  - Service levels
  - Regulatory compliance issues
  - Contractual
  - New products
- \* Measurement of risk through financial impact on depository.
- \* Development of controls.
- \* Business continuity plans.
- \* Corporate insurance against risks such as fraud, neglect, theft, etc.
- \* Money reserves.
- \* Development of recommendations for policies on risk to be approved by the Board.
- \* Periodic review of areas of risk with report on findings to senior management.

PROTECTING PARTICIPANTS AGAINST SETTLEMENT RISK

*Dr. [unclear]*  
*10/10/11*

A major source of risk to depositories, clearing corporations, and ultimately their participants is the failure of other participants. This is generally due to the mutualization of losses among participants as provided for under the rules of depositories and clearing corporations. To date, such losses have been minimal, resulting from the conscious efforts of depositories and clearing corporations to minimize risk.

Today, we will look at steps taken in the risk reduction process, which include:

- . Applicant review/requirements
- . Participant Funds
- . Ongoing monitoring of participants
- . Minimizing risk under a participant financial problem/crisis

While I will talk about how Midwest Clearing Corporation and Midwest Securities Trust Company address these issues, all of the depositories and clearing corporations follow similar procedures.

It should also be noted that I will be speaking about the next-day funds settlement environment. While the basic risk reduction concerns are the same, additional safeguards have been built into the same-day funds environment. You will be hearing about those from Vinnie.

The risk reduction process begins with the application for membership to a depository or clearing corporation. As part of this application, MCC/MSTC requires that the applicant provide certain organizational and operational documents and other

financial information. For a broker/dealer, this includes, but is not limited to:.

- . Financial Reports
  - FOCUS reports for the previous 12 months
  - Audited financial statements for the past two years
- . Partnership agreements or articles of incorporation
- . Disclosures
  - Type of business conducted
  - Insurance fidelity bonds
  - Pending investigation/litigations
- . Broker/dealer forms (how they are registered with the SEC)

For a bank, trust company, or savings and loan applicant, documents and information required are:

- . Reports of Condition (Call Reports)
- . Reports of Income for the past year
- . Annual audited financial statements for the past two years

By reviewing this material, the Market Regulation Department can gain an understanding of how the applicant conducts its business, the experience of the staff, and ensure that minimum capitalization requirements are met.

Where broker/dealers are concerned, the Designated Examining Authority (DEA) for the applicant is also consulted. DEA's are the exchanges and the NASD. They are the first to receive financial statements on the broker/dealers and conduct preliminary reviews. The DEA provides additional insight to the applicant's background, and must also approve the membership of the broker/dealer in a depository or clearing corporation.

Where banks, trust companies and savings and loans are concerned, MCC/MSTC looks to regulators such as the Comptroller of the Currency (OCC), the Office of Thrift Supervision, and the FDIC for background on the applicant.

An applicant may be turned down by MCC/MSTC or the application suspended due to poor financial history (or the lack of same), insufficient capital, or operational deficiencies.

When an applicant is accepted, the Surveillance Department at MCC/MSTC establishes initial deposit requirements for the various Participant Funds. These funds are held by MCC/MSTC to reduce risk from market exposures on trades and/or any other expenses that might be incurred should a participant default on settlement or go out of business. The three funds established by MCC/MSTC for this purpose are:

- . MCC Participant Fund
- . MSTC Participant Fund
- . Trade Guarantee Participant Fund

Minimum deposits for both MCC and MSTC Participant Funds are \$5,000 each although most requirements are significantly higher. Additional contributions are normally based on activity experienced within an account. However, if there appears to be more than normal financial exposure with an applicant, initial deposit requirements may be increased. Separate deposits are maintained for MCC and MSTC to limit risk to participants of each corporation.

Under the Trade Guarantee Program that was established in early 1987, the clearing corporation guarantees settling trades

as of midnight of the day that the trades are reported as compared. For listed issues, this occurs on Trade Date + 1; for OTC issues, on Trade Date + 2. MCC has an agreement with NSCC that establishes these guarantees at the national level.

Once the clearing corporation guarantees a trade, the contra side is satisfied and the clearing corporation assumes the risk. The Trade Guarantee Participant Fund minimizes risk of these future settling trades under this program. Contributions to the fund are based on 102% of the moving 20-day average exposure on future settling trades. (Exposure is the result of market price changes in the securities traded.)

Since contributions to the Trade Guarantee Participant Fund are based on this trading history, deposits to the fund are not usually required of new applicants. However, where projected trade volume is high and/or the type of securities traded pose a risk, such a deposit may initially be required of a new applicant.

Participant Fund minimum deposits must be in cash.

Additional deposits may be in:

- . Cash
- . Government Securities (less than 1 year maturity)
- . Letters of Credit (specific requirements of banks)

While letters of credit are currently acceptable, we do not significantly rely on this form of deposit. The SEC is looking at letters of credit because of the shift in risk to the banks. The issuing bank could refuse to honor the LC, or, worse, the bank could go out of business.

It should be noted that, while losses due to participant failure can be charged against the Participant Funds deposits of all participants in the respective corporation, neither MCC nor MSTC has ever had to do so.

After an applicant becomes a participant, the various participant funds requirements are re-calculated on an ongoing basis.

The financial condition of MCC/MSTC participants is also subject to ongoing monitoring. The Market Regulation Department continues to receive financial reports as filed or prepared by the participant. The Surveillance Department receives various daily reports on critical activity, such as:

- . Value Positions (shorts and longs)
- . Large mark-to-market debits and credits which in themselves reduce risk. Large dollar amounts may signify a problem.
- . Exposure on future settling trades

If a potential problem is determined, the Surveillance Department also has access to all reports available on the account as well as on-line viewing of activity to increase the monitoring level.

Newspapers and trade publications are monitored daily for indications of potential financial or operational problems within a participant. Internal communication is coordinated with Marketing, Participant Services, and the Legal Department, which also coordinates any needed discussions with the SEC.

Watchlists and Flash Reports are produced by both the Market Regulation Department and Surveillance, that report to management on participants having financial difficulty.

There are various levels of financial problems that can occur. Basically, these can be categorized as:

- . Temporary - Firm stays in business
- . Self-Liquidation
- . Forced Liquidation

Under both temporary problems and self-liquidation MCC/MSTC works closely with the participant. Generally, there is not significant exposure to MCC/MSTC in such cases. However, accounts are monitored for unusual activity. Under self-liquidations we also look for an orderly and quick clearance of securities positions from the accounts. We may also have some conversations with the participant's DEA, to confirm temporary financial problems or orderly liquidations.

Where a participant is forced to liquidate, MCC/MSTC increases the monitoring of the account. In such a case, we are usually working with the DEA; acting upon participant requests to move securities only upon approval from the DEA. Occasionally, we may also work with a trustee appointed by SIPC.

In all cases, MCC/MSTC may elect to:

- . Require supplemental deposits to the Participant Funds that cover any increased exposures to MCC/MSTC (calculated daily).
- . Systematically restrict one or more types of activity within the participant account.

In restricting activities, MCC/MSTC may, for example, allow deliveries into an account to clear short positions, but not where inventory will be increased. Depository interface movements and trading activity can also be suspended.

Under MCC/MSTC rules, there are several options available to minimize risk due to a defaulting participant. These options are:

- . Withholding of physical securities withdrawn from a participant's account.
- . Withholding of settlement credits, which is usually done in conjunction with increased or supplemental Participant Funds requirements.
- . Using unpaid for positions as collateral for financing of open debits.
- . Using Participant Funds to pay debits.
- . Advancing the clearing corporation's or depository's own cash.
- . Reversing entries to participants' accounts that generated debits. However, this is a very last resort risk reduction method.

Where the financial collapse of a firm causes major exposure, MCC/MSTC may cease to act for a participant. This situation would more likely occur with a broker/dealer than a bank since banks are usually depository members only. More risk resides on the clearing corporation side, where trades are settled.

Before a decision is made to cease to act for a participant, there are extensive conversations with and between the DEA, our Legal Dept. and senior management. Great care must be taken in ceasing to act for a firm, as the required public announcement may create financial problems for the firm that weren't already there.

Under a cease to act situation, MCC takes steps to clear trading positions quickly, minimizing market risk.

So far, I have addressed how we deal with risk created by participants. It should be noted that exposures can also be created when an issuer of a security held by participants has financial problems. Trading in the security may be halted or the value of the security may be dramatically decreased. When this occurs, MCC/MSTC reviews participant positions in the security to determine what impact this might have on the participant's capital. Calls to the participant and/or their DEA are made to satisfy concerns about risk. Where problems are determined, the same steps to protect MCC/MSTC that were previously outlined are followed.

Where participants are members of multiple depositories and clearing corporations, those organizations have a common interest in those participants. In 1988, the Securities Clearing Group (SCG) was formed by seven of the clearing corporations and depositories to address this issue.

The original seven members were:

- . National Securities Clearing Corporation (NSCC)
- . Depository Trust Company (DTC)

- . Midwest Clearing Corporation (MCC)
- . Midwest Securities Trust Company (MSTC)
- . Options Clearing Corporation
- . Philadelphia Depository Trust Company
- . Stock Clearing Corporation of Philadelphia

In 1990, Boston Securities Exchange Clearing Corporation (BSECC), MBS Clearing Corporation (MBSCC), Participants Trust Company (PTC), and Government Securities Clearing Corporation (GSCC) also joined the group.

The purpose of the SCG is to identify and develop procedures to minimize risks associated with common participants.

The SCG has received SEC approval and members currently exchange appropriate information when common participants are having financial problems. An automated information database that will include critical financial data on common participants is currently under development. Daily updates are planned with access to the database by SCG members based on their common participants.

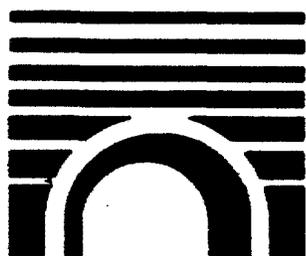
↓ In summary, the steps taken by MCC/MSTC to minimize risk in the depository and clearing corporation and, therefore, reduce risk to participants are:

- . Screening of applicants
  - Review of financial history
  - Operating practices
- . Participant Funds
  - Standard
  - Supplemental

- . Ongoing monitoring
- . Watchlists
- . Restriction/Suspension of activity
- . Withholding of credits
- . Right to reverse
- . Ceasing to act for a participant
- . Participation in SCG

Midwest Securities Trust Company

Midwest Clearing Corporation



**PARTICIPANT  
APPLICATION  
QUESTIONNAIRE**

## MCC/MSTC PARTICIPANT INFORMATION

*This form must be completed by the Participant and returned to:  
Product Manager, Room 2100*

Firm Name:

Address:

City, State, Zip

Telephone Number:

Corporation:

Partnership:

Tax ID Number:

Nominee Name:

President/Executive Officer:

Operations Manager:

Financial Officer:

EDP Manager:

Settlement Bank for MCC Account:

Account Number:

Contact for Daily Settlement Figures:

Phone Number for Contact:

Daily Delivery Instructions:

Purlator \_\_\_\_\_ First Class Mail \_\_\_\_\_ Brinks \_\_\_\_\_ Express Mail \_\_\_\_\_ Other \_\_\_\_\_

Contact for bi-monthly Audit Package:

Contact for Ominbus Proxy Information:

Service Bureau:

Exchange Memberships:

**BUSINESS PROFILE**

Please Check (✓) the appropriate box.	
<b>EQUITIES:</b>	
Listed	Floor Broker
OTC	Market Maker
Foreign Issues	
Options	Floor Broker
Corporate Bonds	Municipal Bonds
Broker Dealer	Dealer
Investment	
<b>UNDERWRITINGS:</b>	
Syndicate Member	Selling Group
<b>EQUITY</b>	
Listed	OTC
Corporate Bond	Municipal Bond
<b>COMMERCIAL PAPER</b>	
Dealer	Broker
Issuing Agent	
<b>GOVERNMENTS</b>	
<b>MORTGAGE BACKED SECURITIES</b>	
<b>COMMODITIES</b>	
<b>FUND MANAGER</b>	

Name of Participant Applicant: \_\_\_\_\_

Address of main office: \_\_\_\_\_

**I BACKGROUND INFORMATION**

1. Form of Organization

Corporation \_\_\_\_\_  
Partnership \_\_\_\_\_

2. Date Business Started: \_\_\_\_\_

3. Designated Examining Authority: \_\_\_\_\_

4. Exchange Memberships: \_\_\_\_\_

5. Other Memberships: \_\_\_\_\_

6. Briefly describe any recent membership changes as well as those contemplated during the next six (6) months.

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

7. Chief Executive Officer: \_\_\_\_\_

8. Financial Officer: \_\_\_\_\_

9. Operational Officer: \_\_\_\_\_

10. Number of registered representatives: \_\_\_\_\_

11. Number of operational personnel: \_\_\_\_\_

12. Number of branch offices: \_\_\_\_\_

153

13. Name of outside counsel: \_\_\_\_\_

14. Name of accounting firm: \_\_\_\_\_

15. Date of last annual outside audit: \_\_\_\_\_

16. Date of last inspection by Designated Examining Authority: \_\_\_\_/\_\_\_\_/\_\_\_\_

17. Is SEC Registration currently effective? Yes \_\_\_\_ No \_\_\_\_

18. Method of Recordkeeping

Manual: \_\_\_\_\_

Computer: \_\_\_\_\_ (in-house)

Other: \_\_\_\_\_

19. If a Service Bureau is used, give name and address:

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

20. Location of books and records if other than Main Office:

\_\_\_\_\_

21. If Participant/Applicant is affiliated with, controls, and/or is controlled by any other business entity, describe details of relationship:

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

154

22. List major banking relationships and available lines of credit:

---

---

---

---

---

23 (a) Briefly describe and list any clearing arrangements or agreements. (State if Participant/Applicant is self-clearing, a clearing broker, or clears through others. Provide a list of those broker-dealers involved and identify the type of securities being cleared, i.e., listed, OTC, options, etc.)

---

---

---

---

---

(b) Briefly describe any changes contemplated in Participant/ Applicant's clearing arrangements.

---

---

---

---

---

---

155

**II**      **TYPE OF BUSINESS CONDUCTED**

1      (a)      Check, in appropriate box, types of business engaged in (or to be engaged in if not yet active) by Participant/Applicant. Do not check any category which accounts for or is expected to account for less than 10 percent of annual gross revenue from the securities or investment advisory business.

- Exchange member engaged in exchange commission business.
- Exchange member engaged in floor activities.
- Broker or dealer making inter-dealer markets in corporate securities over-the-counter.
- Broker or dealer retailing corporate securities over-the-counter.
- Underwriter or selling group participant (corporate securities other than mutual funds).
- Mutual fund underwriter or sponsor.
- Mutual fund retailer.
- U.S. Government securities dealer.
- Municipal securities dealer.
- Municipal securities broker.
- Broker or dealer selling variable life insurance or annuities.
- Solicitor of savings and loan accounts.
- Real estate syndicator.
- Broker or dealer selling oil and gas interests.
- Put and call broker or dealer option writer.
- Broker or dealer selling securities of only one issuer or associated issuers (other than mutual funds).
- Broker or dealer selling securities of non-profit organizations (e.g., churches, hospitals).
- Investment advisory services.
- Broker or dealer selling tax shelters or limited partnerships.
- Stock borrowed.
- Other (Give Details) \_\_\_\_\_

(b)      Briefly describe any changes contemplated during next six (6) months in the Participant/Applicant's business.

---

---

---

(c) Does Participant/Applicant effect transactions in commodity futures, commodities, or commodity options as a broker for others or dealer for its own account?

Yes \_\_\_\_\_ No \_\_\_\_\_

(d) Does Participant/Applicant engage in any other non-securities business? (If "Yes", describe each such other business briefly).

Yes \_\_\_\_\_ No \_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_

2 (a) Record sources of Participant/Applicant's income during most recent twelve (12) month period.

\_\_\_\_\_ %  
\_\_\_\_\_ %  
\_\_\_\_\_ %

(b) Projected changes in the sources of income.

\_\_\_\_\_  
\_\_\_\_\_

3. Securities accounts for customers:

Approximate number of active accounts

Cash \_\_\_\_\_  
Margin \_\_\_\_\_

Clientele

Retail \_\_\_\_\_  
Institutional \_\_\_\_\_  
Wholesale \_\_\_\_\_

Types of Accounts

Discretionary \_\_\_\_\_  
Investment Advisory \_\_\_\_\_  
Other (specify) \_\_\_\_\_

4. Approximate number of monthly tickets: \_\_\_\_\_

5. Market Making Activities

Does Participant/Applicant make markets?

Yes \_\_\_\_\_ No \_\_\_\_\_ OTC # \_\_\_\_\_ Listed # \_\_\_\_\_

Other markets, describe: \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Price range of securities \_\_\_\_\_  
\_\_\_\_\_

Does Participant/Applicant act as correspondent for another broker-dealer?

Yes \_\_\_\_\_ No \_\_\_\_\_

If yes, for whom? \_\_\_\_\_

Does another broker-dealer act as correspondent for another Participant/Applicant?

Yes \_\_\_\_\_ No \_\_\_\_\_

If yes, who? \_\_\_\_\_

List any current relationships.  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

158

6. Underwritings

Number currently in registration: \_\_\_\_\_

Number in process of registration: \_\_\_\_\_

Number completed within last twelve  
(12) months as a sole underwriter: \_\_\_\_\_

Number completed within last twelve  
(12) months as a selling group member: \_\_\_\_\_

Average offering price of those in registration: \_\_\_\_\_

Average offering price of underwriting completed: \_\_\_\_\_

Types of Underwritings: Bonds \_\_\_\_\_ % Stocks \_\_\_\_\_ %

III. BONDING

Is Participant/Applicant required to have a fidelity bond?

Yes \_\_\_\_\_ No \_\_\_\_\_

Name of Insurance Company: \_\_\_\_\_

Fidelity	\$	_____
On Premises	\$	_____
In Transit	\$	_____
Misplacement	\$	_____
Forgery and Alteration	\$	_____
Securities Loss	\$	_____
Fraudulent Trading	\$	_____
Amount of Deduction Provision	\$	_____

Expiration date of bond: \_\_\_\_ / \_\_\_\_ / \_\_\_\_

Is there a cancellation rider? Yes \_\_\_\_\_ No \_\_\_\_\_

Briefly describe the circumstances of any claims paid during the previous 24 months.

---

---

Briefly describe any changes contemplated in Participant/Applicant's bonding coverage.

---

---

---

**IV PENDING INVESTIGATION(S) AND/OR LITIGATION**

For purposes of this Section IV, "control" means the power, directly or indirectly, to direct the management or policies of a company, whether through ownership of securities, by control or otherwise. Any person that (i) is a director, general partner or officer exercising executive responsibility (or having similar status or functions); (ii) directly or indirectly has the right to vote 25% or more of a class of a voting security or has the power to sell or direct the sale of 25% or more of a class of voting securities; or (iii) in the case of a partnership, has the right to receive upon dissolution, or has contributed, 25% or more of the capital, is presumed to control that company.

1. Please list any legal or administrative proceedings pending against the Participant/Applicant, any officer or partner of Participant/Applicant, or any other person or organization that directly or indirectly controls, or is under common control with the Participant/Applicant brought by the SEC, state securities agencies or self-regulatory organization.

---

---

---

2. Please list any orders or sanctions entered against the Participant/Applicant, any officer or partner of Participant/Applicant, or any other person or organization that directly or indirectly controls, or is under common control with the Participant/Applicant by any courts, the SEC, state securities agencies, or self-regulatory organizations which affect the Participant's securities business.

---

---

---

3. Please list any other federal or state investigations or proceedings involving the Participant/Applicant, any officer or partner of Participant/Applicant, any other person or organization that directly or indirectly controls, is under common control with the Participant/Applicant or any of its affiliates which may have an effect on the Participant's securities business.

---

---

---

4. Please furnish the details of any pending lawsuit(s) resulting in contingent liabilities that may affect business operations or net capital.

---

---

---

**DATE:**

---

**SIGNATURE:**

---

---

**A Bankwide Assessment of Risks Associated With  
Traditional and Non-Traditional Services  
and New Business Opportunities**

**RISK ASSESSMENTS:  
THE RISK MANAGEMENT PROCESS**

By H. Felix Kloman  
and  
Douglas G. Hoffman



AMERICAN  
BANKERS  
ASSOCIATION  
1120 Connecticut Avenue, N.W.  
Washington, D.C. 20036

1622

---

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional service. If legal advice or other expert assistance is required, the services of a competent professional person should be sought.

—From a Declaration of Principles jointly adopted by a Committee of the American Bar Association and a Committee of Publishers and Associations.

---

Copyright © 1984  
American Bankers Association  
All rights reserved. This book may not be reproduced in whole or in any form whatsoever without permission from the publishers.

Printed in the U.S.A.

---

# Acknowledgments

Mr. Kloman is President and Director of Risk Planning Group, Inc., in Darien, Connecticut. The firm undertakes risk and insurance studies for corporations, governmental bodies and educational institutions, as well as banks and financial organizations. He is Editor of "Risk Management

Reports," Publisher of "Government Risk Management Reports," and serves on the Editorial Advisory Board of "Risk Management" magazine.

Mr. Hoffman is Senior Consultant of Risk Planning Group, Inc. He is Editor of "Bank-Risk: the Bank Risk Management Quarterly."

---

# Foreword

Dear Colleague:

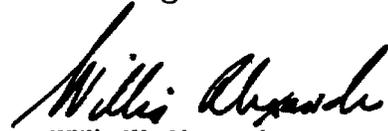
Dealing with risk is a part of the life of every business, but this is especially true for banks. The very nature of banking creates unique types and levels of risk. In addition, the growing sophistication of operations linked to the banking industry's diversification into related financial services exposes banks to types of risk not experienced in the past.

Your fellow bankers who serve on ABA's Banking Professions Council recognized the need for a management tool which will help the industry to identify, analyze, and control the risks associated with a changing banking environment. As such, the Council commissioned a major ongoing bank-wide assessment of risk associated with tradi-

tional and non-traditional services and new business opportunities.

The result of these assessments will be reports such as this one distributed as an ongoing membership service which will help you and your bank to better assess and manage your risks, both existing and emerging.

Reliance upon this risk management process, as a legitimate management tool for protecting a bank's assets, may well determine the success of any banking institution, its profitability, and the continuation of public confidence, which is the cornerstone of banking.



Willis W. Alexander  
Executive Vice President  
American Bankers Association

165

---

---

# Risk Management

## INTRODUCTION

These are times of increasing uncertainty for the bank chief executive officer. Events of the past several years, including Drysdale Securities, Penn Square, the Butcher banks, and the international debt bomb, may be beginning to affect the public confidence which is the keystone of America's banking system. Consider also these events:

- A western bank's failure is caused in part by its inability to recover funds paid out under standby letters of credit.
- In the Southeast, a bank customer is murdered at night at an ATM. The bank is sued for wrongful death.
- A bank is sued for failure to disclose adverse financial information on one customer to another customer who continued to supply the first customer while assuming the bank would advise it in the event of financial difficulty.
- Because of a delayed wire transfer of \$27,000 to a bank customer, a business deal was cancelled. The customer then sued the bank for \$2.1 million and won.

With increasing demands for non-interest income and for taking advantage of new opportunities, many banks appear to have introduced new services in response to these competitive and/or market pressures with too little regard for some of the potential short-term and long-term risk problems. The question is not only one of

the very real financial loss to the bank itself, but also of the potential loss of esteem which banks, in general, hold in the United States. As symbols of financial trust, banks are responsible not only to their customers and employees, but to the public for maintaining both the image and reality of fiscal solidity and conservation. With increasing competitive pressures and reduced regulatory limitations, the ability of the bank chief executive officer (CEO) and senior management to respond intelligently to increased uncertainty may be more, rather than less, difficult. While it is obvious that bank stability and operating continuity are essential for the future, rapid economic, technological and political changes tend to undermine that stability.

The bank CEO is thus, in a sense, the overall "risk manager" for any financial institution, the person responsible for stimulating an in-depth awareness of the changing, growing and interrelated risks which could materially affect the bank, and for initiating appropriate and prudent corrective action. While senior management can be delegated the task of reviewing new products and services, what may be required today is a new functional responsibility, entitled "risk management," to enable the CEO and senior management to assure customers and the Board alike of the ability of the bank to provide continuity of service with profitability.

The risk management discipline, a practical approach to addressing this responsibility, has evolved over the past decade as a technique of increasing importance to bank CEOs in the conservation of

bank resources against the effects of unexpected, accidental, or adverse events. As such, risk management is as important to a bank's continued success and to public confidence as the profitability of its operating divisions. Indeed, it can be shown that successful risk management can make a dramatic contribution to improved earnings.

The roots of today's risk management discipline are diverse. One can be found in the increasing sophistication of management methodology, responding to the growth and complexity of modern organizations. Henri Fayol, writing in the early years of this century, argued that management is made up of seven elements, one of which is security management. "Security" can be defined as protecting the assets of an organization, including its ability to continue operations. It is a key element of any strategic plan.

Another root may be found in the more recent development of sophisticated analytical techniques for assessing macro risks, such as nuclear disaster and earthquake. As these techniques developed by quasi-governmental think tanks and academic researchers have been created, improved and modified, they have been increasingly applied to other forms of risk with encouraging results.

Finally, one of the deepest roots may be found in insurance, a centuries-old method of risk funding and risk spreading in such traditional areas as criminal activity, loss of or damage to property and third-party liabilities.

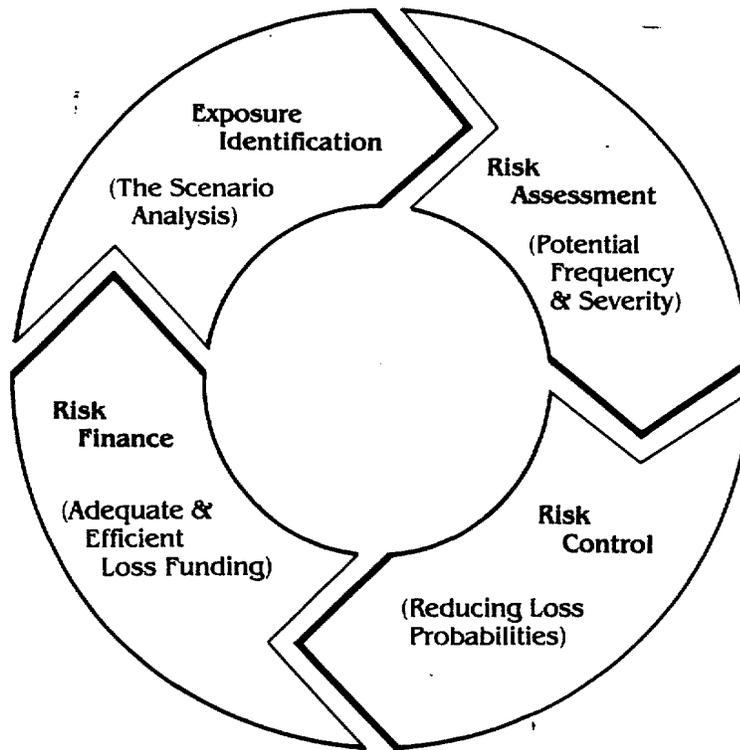
Today, with the vagaries of an ever-changing world, the risk management discipline is beginning to address not only traditional risks but also many non-traditional risks as well. Unfavorable political activity, terrorism, currency fluctuation, interest rate volatility, and employment discrimination are among some of the more important newer and non-traditional risks that are examples of uncertainty with which we have to deal. For example, electronic funds transfer systems, contingent (off-

balance-sheet) liabilities, automated teller machines, the advent of electronics to retail banking, and the entry of banks into the securities business have all raised new forms of risk which must be accurately assessed.

Senior bank officers have therefore recognized that the orderly process of a risk management discipline has the capacity of assisting them in the management of all aspects of uncertainty regarding unexpected or accidental events. In a sense, a failure to adopt the risk management process could lead to an inability to respond to changing events, and to the failure of the bank. There is also a growing recognition of the interrelationship of all forms of risk. It is equally evident that risk also creates opportunity. A proven capability to respond to an unexpected event can enhance professional reputation and public confidence. Today, the risk management function within a bank is being expanded so that it can be intelligently applied to both traditional and non-traditional risk areas. It is being seen more clearly as a logical decision-making process, one which can and should be an integral part of the strategic and tactical plans of a bank, to identify and assess risks of loss and to select the most advantageous treatment measures. The process can be seen as a circle (Figure 1) of interrelated and continuing steps, including:

1. *Exposure Identification:* The creation of a continuous discovery process to identify the resources for which a bank is responsible and the loss exposures which could materially affect them. This is, in effect, a continuing "scenario" analysis in which the question "what if" is being put, again and again, by operating officers to the changing operating conditions.
2. *Risk Assessment:* The measurement of financial risk in terms of past and future frequency and severity of both individual and cumulative losses.

**Figure 1**  
**Administering the Risk Management Process—**  
**A Systematic and Continuing Effort**



3. **Risk Control:** The application of appropriate and prudent techniques for reducing or eliminating risk or loss through proven and cost-effective procedures. Contingency planning is one of the most important elements of risk control.
4. **Risk Finance:** The provision of sufficient funds to meet loss situations as and if they occur, by use of both internal and external financial resources, including insurance.
5. **Administration:** The development of administrative techniques to carry out a risk management program most effectively within the bank. This requires not only senior management commitment but also the awareness of risk and participation in risk control by operating officers.

Successful administration of risk management also requires the adoption of a clear policy by the Board of Directors, the designation by the CEO of one or more persons to take responsibility for the function, the active involvement and interest in the process by operating personnel and, finally, a system of performance measurement in periodic reports to the Board.

The growing maturity of the risk management function and the dramatic expansion of banking activities into the broader financial service arena indicate an enlarged role for risk management. It recognizes that risk has positive as well as negative connotations and that, to reduce the negative results and enhance profit potential, management will require a more formal and logical approach to today's and, more importantly, tomorrow's risks.

## EXPOSURE IDENTIFICATION

The first step in risk management is to identify both bank resources and the exposures to loss which could materially affect them. In particular, with the extension of bank activities into new financial service areas, it is of increased importance to review carefully new forms of property and new responsibilities to customers.

Resources may be classified as:

1. *Physical*: Real and personal property which the bank owns or for which it may be legally responsible.
2. *Human*: The skilled people who are essential to the continuation of banking and financial services, both inside and outside the bank.
3. *Financial*: The capital, deposits, and collateral on which the banking system rests.
4. *Intangible*: Difficult-to-value resources, such as communications media (mail or telecommunications), adequate transportation, and EFT systems, for example.

Loss exposures may be classified as:

1. *Non-Traditional*: Political risk in all its forms (expropriation, devaluation, confiscation, terrorism, etc.); the flow of funds electronically from location to location and across national borders; the rapid growth of automated teller and "point of sale" machines. The expansion of financial services to such areas as discount brokerage, financial counselling, and, potentially, insurance and underwriting of public securities will inevitably create new forms of risk.
2. *Natural*: "Acts of God," such as earthquake, flood, windstorm and tornado.
3. *Direct*: Such incidents as crime in its various forms (internal and external), fire, explosion, collision, transporta-

tion risks, vandalism, and malicious mischief.

4. *Indirect*: The consequential financial results of other events (direct, natural, human, liability) which reduce earnings or cash-flow or force the expenditure of additional funds.
5. *Human*: Death, disability, accidental injury, sickness, or old age.
6. *Third-Party Liabilities*: The potential financial losses arising out of unintentional or intentional torts, statutory liabilities and contractual liabilities. A growing litigious society, inflation, and changing social values indicate a steadily worsening situation. One of the most serious new liability areas is that of professional liability. A number of recent cases have created precedents for the imposition of liability against bankers who fail to discharge their obligations in a professional manner, through either error or omission.

These loss exposures are elusive and constantly changing, requiring a bank risk management officer to apply sophisticated risk discovery techniques in an alert and intelligent manner, on a continuous basis. They also require that all bank officers have an appreciation and understanding of the goals and objectives of the risk management function. Neither the responsible CEO nor the risk management officer alone can accomplish the goal of being prepared for adverse events. Each officer within the organization must be trained in risk awareness and in responsibility for risk control.

## RISK ASSESSMENT

It is not enough to identify a critical resource and the exposures to loss which could affect it. Financial risk must be assessed by determining frequency and severity probabilities. Some loss exposures are inconsequential in nature while others

are potentially catastrophic. At the same time, a very high frequency of small losses can create a cumulative impact of some significance, while a potentially catastrophic event with a miniscule probability of occurrence may well be disregarded.

Each resource carries a value, a function of time and economic conditions. The value of any resource is based on a dynamic interrelationship between its market or replacement value and, perhaps more importantly, the income, earnings or cash flow which may be generated by it. Loss of use of a resource may be far more costly than its physical replacement value.

The assignment of probabilities for loss frequency and severity requires a thorough understanding of a bank's own past loss experience, a reliable extension of this experience into the future, and, where data are lacking, an appreciation of the experience of others and an ability to fit rapidly changing conditions to these probabilities. Decision-trees, computer modeling, Monte Carlo simulations and Delphi techniques all may play a role in the risk assessment process of a sophisticated bank risk management function. Loss forecasting then becomes a major responsibility, for both current and proposed operations.

Risk assessment, like exposure identification, is a continuing process. In some areas of risk, especially the non-traditional, precise measurement is impossible, but a range of probabilities can be used to express degrees of risk. The process is also important in bank planning. Strategic planning requires an appreciation of risks as well as rewards: risk management can provide the former and assist in realizing the latter.

## **RISK CONTROL**

The interrelationship of the steps of the risk management process is most clearly apparent in risk control, the elimination and/or reduction of loss and risk. Risk assessment points to those areas where

corrective action should be undertaken. Risk control is the process of developing that action, through policies, applying procedures for control and providing constructive assistance to operating areas so that risk can be brought within manageable boundaries. One of the major problems found in most banking institutions is that risk control is administratively fragmented, with line responsibility often given to different departments. In the future, the coordination of risk control activities will almost certainly contribute to better risk management, reduced losses and a direct improvement in return on equity.

Today, the pressure points of risk control within a banking institution may include the Asset-Liability Committee, the Audit Department, and the Audit Committee of the Board, the Credit Committee, the Compliance Officer, the Operations Manager, and the Security Officer.

In the future there will be greater coordination among these individuals and groups in applying prudent risk controls. The two most important areas will be:

1. *Contingency Planning:* This is rapidly becoming one of the most important areas of risk control, focusing pre-event, event, and post-event responses for risks in the data processing center, trust operations, and electric funds transfers. Some planning concepts are now being applied to all operational areas of the bank, under the heading of "business recovery" or "crisis management."
2. *Security:* The legislative and regulatory mandates of the Bank Protection Act of 1968 and Regulation P of the Federal Reserve System stipulate the minimum required policies, procedures and physical protection for most banking institutions. The law, however, is generally a reflection of past conventional wisdom and prudent practice, not necessarily an appropriate response to current and

future conditions. Banks today have limited statutory guidance in developing appropriate risk control responses for charge card, data, and electronic funds transfer system security.

Other risk control concerns include:

1. *Personnel Safety:* National and state occupational safety and health standards set minimum requirements for work safety, the work environment and record keeping. Beyond these, there is, as well, increasing concern and effort about the safety and health of bank employees off the job (e.g. employee wellness programs).
2. *Property Protection:* The physical assets of a banking institution should be properly protected against the direct results of such events as fire, windstorm, earthquake, etc. Critical records, hardware and software are the major concerns.
3. *Other Elements:* A major activity of bank risk management is that of reviewing the many contractual relationships that a bank has with other organizations, to assure that mutual responsibilities and liabilities are appropriately delineated and understood, and that proper financial resources back up these responsibilities. Risk control responsibilities also include the development of policies and procedures for the safe operation of bank-owned or leased automotive vehicles and, where applicable, aircraft and watercraft, and for the development of procedures to assure that the bank is not involved in any environmental pollution.

The risk management function is extending its responsibility in the non-traditional risk area. A major control mechanism is the continuing education of loan, trust, and other operational officers so that they appreciate and understand the wide variety of loss exposures that face the bank and

bank customers. An effective working relationship between bank risk management and audit departments is also essential, as auditors are frequently the first point of contact with new and changing loss exposures.

Flow charts defining loss exposures, risk assessment and risk controls have been in use in a number of banks for some time. Figures 2 through 4 are analyses of risk in three non-traditional operating areas—discount brokerage activities, wholesale payment systems mechanisms and ATM systems.

## RISK FINANCING

A well-managed bank will assure itself of the ready availability of sufficient funds so that, after any conceivable loss, it can continue to serve its customers and depositors, as well as maintain a reasonable return to its shareholders. Some of these funds will be internal reserves, some may come from lenders, such as the Federal Reserve system, and some may come from insurance companies. Despite the most thorough and well planned exposure identification, risk assessment and risk control programs, unforeseen events can still occur. It is in this area that innovative risk financing programs are essential. The objectives of risk financing are as follows:

- Make the best use of the total funding sources available to the bank. For example, retain internally the funding of those losses which are relatively predictable, and transfer to others the losses that are more unpredictable and potentially catastrophic.
- Provide sufficient funding, in terms of total financing available, to meet the worst possibility of loss events (individually or cumulatively). Plan for a catastrophe.
- Strive to stabilize, as much as practical, risk funding costs over time, avoiding excessive peaks and valleys.

**Figure 2**  
**Discount Brokerage Activities**

Operational Loss Exposures	Risk Assessment	Risk Control
<i>Discount Brokerage Activities:</i>		
Financial and liability exposures arising out of financial and securities trading acting as a carrying, clearing or introducing broker or operating under a contractual arrangement with a registered broker.		
<i>Areas of Concern:</i>		
<ul style="list-style-type: none"> <li>Physical damage to operations.</li> </ul>	Fire, flood, windstorm, etc.	Fire suppression equipment and other protective devices.
<ul style="list-style-type: none"> <li>Loss of income/customers arising out of interruption of services.</li> </ul>	Power outage; loss of telecommunications; fire; other "Acts of God."	Application form/legal agreement, back-up/contingency plans.
<ul style="list-style-type: none"> <li>Legal liabilities for errors or omissions in services.</li> </ul>	Improper or illegal advice, improper release of information, improper execution, errors in customer accounting.	Written confirmation on all transactions, maintenance of ledgers, retention of customer correspondence, training, "reasonable diligence" requirement.
<ul style="list-style-type: none"> <li>Availability of key personnel and their skills.</li> </ul>	Death, disability, leaving employment. (Risk will diminish as activities grow.)	Contractual affiliation with registered broker: written agreement.
<ul style="list-style-type: none"> <li>Damage to credibility and reputation of the bank.</li> </ul>	From all of above exposures.	Use of proven brokers; NYSE net capital and insurance requirements; insolvency protection of SIPC.

**Figure 3**  
**Wholesale Payments Systems Example Risk Assessment Model**

Operational Loss Exposures	Risk Assessment	Risk Control
<i>Wholesale Payments Systems:</i>		
Financial loss to or liability of bank through use of electronic funds transfer (EFT) systems, such as FedWire, CashWire, CHIPS and corporate-to-corporate ACH.		
<i>Average Values (1983):</i>		
	FedWire: \$2.1 million	
	CashWire: \$200,000	
	CHIPS: \$3 million	
<i>Areas of Concern:</i>		
<ul style="list-style-type: none"> <li>Fraud.</li> </ul>	Fraudulent requests, alteration of valid request; damage/destruction of records. (EFT not covered under UCC.)	Authentication codes (encryption in future); call-back procedures; wire room security (hardware and software); special audits; legal customer agreements.
<ul style="list-style-type: none"> <li>Operating Errors.</li> </ul>	Failure to initiate transfer; wrong amount or beneficiary; duplication of transfer.	Logging and balancing; operator training; call-back procedures; account reconciliation/suspense accounts.
<ul style="list-style-type: none"> <li>Credit Exposure (Funds transfers are immediate and irrevocable: FedWire).</li> </ul>	Loss of principal; loss of earnings; consequential damages.	Some end of day "unwinding" possible. Other controls: —bi-lateral credit limits —credit cap FedWire: risk substantially absorbed by Fed.
<ul style="list-style-type: none"> <li>Service Disruption.</li> </ul>	External: power outage, flood, earthquake, fire. Internal: failure of hardware, software (loss of earnings; loss of customer; market dissatisfaction).	Duplication of facilities; alternate network capability; contingency plan (training; testing).

**Figure 4**  
**Automated Teller Machine Systems**

Potential Loss Exposures	Risk Assessment	Risk Control
<i>Overall ATM System</i>		
Loss of market share and competitive positioning, direct financial loss to customer and/or bank, inadequate and ineffective risk assessment/management.		
<i>Areas of Concern:</i>		
• Strategic or marketing risk.	—Failure to offer may mean erosion of market share.	—Develop a strategy that addresses potential credit, issuance and maintenance risks.
• Risk of financial loss.	—Consumer problems include stolen cards, counterfeiting, overdrafts, and bogus deposits.	—Cardholder insurance criteria, usage control procedures and education programs are essential.
• Technology risk.	—Obsolescence of hardware and software, availability of original vendor, systems compatibility and security risks need to be assessed.	—A combination of careful planning, common sense and diligent attention from senior management are needed to deal with technology risk; indeed, a broad business perspective with attention to issues such as vendor reliability, upgradability, compatibility, systems integrity and maintainability must be applied.
• Physical security.	—Burglary, robbery and vandalism top the list followed by malfunction, bodily injury to customers and fire.	—Sound machine security (construction, alarms, surveillance), environment security (location, lighting, housing) and control procedures (servicing controls, audit trails, repair supervision) are needed.
• Data security.	—Unauthorized access is generally considered the greatest risk. Also of concern are privacy, systems errors and inter-institution ramifications.	—Systems must be designed to limit access to on-line data bases and/or communications systems (PINs, encryption, key management), proper backup systems for on-line down time must be in place, network controls and software security programs should be developed.

- Take maximum cash flow advantages in the operation of risk funding plans, since a bank should be able to generate a higher return on these funds than other financial institutions.
- Obtain the lowest reasonable direct cost of risk financing, commensurate with the funds that are made available and the services that are offered by funding media.<sup>2</sup>

A key step in developing a risk financing program is a definition of the bank's capacity for retaining risk and/or loss. This

should be expressed not only as a maximum amount that the bank can accept in a single occurrence but, perhaps more importantly, also as a maximum sum which can be cumulatively absorbed in a single fiscal year. This risk retention capability, per occurrence and aggregate, will change from year to year as a bank's fortunes change. It, therefore, should be appropriately and periodically modified.

While in the past many bank risk financing programs have displayed an over-reliance on insurance as a primary funding tool, and a means of transferring risk, today most larger banks appear to be

substantially self-funded for some 50-70% of their accidental losses. Smaller banks are now beginning to accept higher deductibles and greater levels of risk retention. Captive insurance companies are also under study as possible future financing options. Insurance, however, remains a frequently used method of handling major risks of accidental loss, and sophisticated bank risk managers are pressing the worldwide insurance industry to provide more catastrophe insurance for areas of non-traditional risk. The insurance marketplace, both U.S. and foreign, has begun to respond more imaginatively to these new non-traditional funding requirements, especially as sophisticated risk managers explain risks, and their controls, more persuasively to the market.

## ADMINISTRATION

The practice of the risk management discipline within a banking institution requires continuous direction, generally by an individual officer specifically assigned this task. Because of the range of both traditional and non-traditional risks, there is an increasing stress on the *function* of risk management, rather than on an individual *person* or position, inasmuch as many of the responsibilities can and indeed must be shared among different operating officers. For example, while security is an important risk management responsibility, the law mandates a separate "security officer." Personnel safety is a risk management responsibility, but personnel or human resource officers will often have primary responsibility for all relationships with employees. In the larger bank, generally one with over \$500 million in deposits, there will be a full-time risk management officer. In a smaller institution, risk management will necessarily be a duty in addition to others, often the responsibility of the Controller, Security Officer, or Operations Officer. The key to organization of a successful risk management program is in

the designation of a single officer to coordinate the program, to prepare and gain approval by the Board of a written statement or policy on risk management, and to maintain effective and continuing communications with the operating departments.

Given the range of risks inherent in the banking environment, bank risk management will require, under the leadership of the CEO, the active participation of a risk management officer, an asset/liability officer, a strategic/long-range planning officer, an auditor, and legal counsel. Other activities will also play a role in the risk management process including security, insurance, personnel, data processing, retail banking, commercial banking, and operations.

A clear and simple statement of policy is an essential prerequisite for an effective program. In the larger banks, this will be approved by the Audit Committee of the Board; in the smaller banks by the Board itself. The following wording is an example of a policy that can be adapted for a bank's use:

"The Bank and its subsidiaries shall be protected against accidents or losses which, in the aggregate during any financial period, would significantly affect personnel, property, income, or the ability of the bank to continue to fulfill its responsibilities to its depositors, customers, shareholders, employees and the public.

"To all these risks of accidental loss the Bank will apply the risk management process, which includes a systematic and continuous identification of loss exposures, assessment of risks in terms of frequency and severity probabilities, the application of prudent risk control procedures, and the financing of risk consistent with the Bank's financial resources.

"The Board of Directors will have the final responsibility of assuring that a prudent risk management program is

in effect at all times. A review of the program, including risk assessments, risk controls, and risk financing procedures shall be undertaken by senior management on behalf of the Board of Directors at least annually and the minutes of meetings shall indicate the date of review and the Board's approval.

"The administration of the Bank's risk management program, including coordination of risk control efforts, is assigned to, and directed by the Risk Management Officer."

The broad responsibility of the bank risk management officer, and the function of risk management, will include the elements of exposure identification, risk assessment, risk control and risk funding, plus more specific duties such as the review of major leases and contracts, participation in strategic planning (reviewing the risks in new activities), review of major loans and lease financing, coordination with internal audit, security liaison with data processing, coordination with personnel or human relations on the design and funding of certain benefit programs, and maintenance of essential records.

A key responsibility will be to establish and maintain effective lines of communication with all bank personnel, to enhance their awareness of current and new operating risk and loss exposures. Communication will also include periodic seminars

for various bank employees and an annual report to the Board or Audit Committee. In this regard, banks are beginning to use "cost of risk" for annual performance measurement. Cost of risk is the sum of risk control expenditures; internally funded (self-insured) losses; external funding costs (FDIC and other insurance premiums); and administrative costs.

Cost of risk is compared to assets, deposits and other measures of bank operations and growth, to permit comparative analysis among banks and with other organizations.

## CONCLUSION

The risk management discipline is still evolving and developing, particularly within the financial services industry environment in the United States. There is no doubt, however, that it has a major role to play in its application to the non-traditional risks arising out of new financial services as well as to those which have been traditionally considered through insurance contracts. The success of the application of the risk management process to non-traditional risk areas may well determine the success of a bank, the size of its earnings and return on equity, and the continuation of public confidence, which is the cornerstone of banking.

A failure on the part of financial institutions to better manage many of these risks could result in legislative and regulatory controls being imposed on the industry.

# Risk Assessment Tear-out Order Form

To order additional copies of this publication, or others in the *Risk Assessment* series, simply tear out and complete this order form and mail it with payment to ABA's Order Processing Department.

For additional information on the *Risk Assessment* series, and new editions of the series that may not be listed on this order form call (202) 467-4047.



## Order Form



ORDER PROCESSING DEPARTMENT  
American Bankers Association  
4-B Industrial Park Drive  
Waldorf, Md 20601

Check enclosed. (Processing/invoicing charges will be added to orders not accompanied by remittance.) Non-members must pre-pay. All rush orders will be charged 10% of the total value of the order whether or not pre-paid. Prices are subject to change without notice.

Quantity	Catalog Number	Title of Publication	UNIT COST		Total
			Price	ABA Member Discounted Price	
	215301	Risk Assessment: The Risk Management Process (Overview)	\$15	\$10	
	215302	Discount Brokerage Services	\$22.50	\$15	
	215303	Automated Teller Machines	\$22.50	\$15	
	215304	Wholesale Wire Payments Systems	\$22.50	\$15	
	215300	Complete Risk Assessments Series (includes all four above named publications & binder)	\$67.50	\$45 <sup>1</sup>	
<b>GRAND TOTAL</b>					

(PLEASE PRINT)

Name \_\_\_\_\_  
 Title \_\_\_\_\_ Bank \_\_\_\_\_  
 Street Address \_\_\_\_\_  
 City \_\_\_\_\_ State \_\_\_\_\_ Zip \_\_\_\_\_  
 Signature \_\_\_\_\_

8491-5-77-077-01

## Order Form



ORDER PROCESSING DEPARTMENT  
American Bankers Association  
4-B Industrial Park Drive  
Waldorf, Md 20601

Check enclosed. (Processing/invoicing charges will be added to orders not accompanied by remittance.) Non-members must pre-pay. All rush orders will be charged 10% of the total value of the order whether or not pre-paid. Prices are subject to change without notice.

Quantity	Catalog Number	Title of Publication	UNIT COST		Total
			Price	ABA Member Discounted Price	
	215301	Risk Assessment: The Risk Management Process (Overview)	\$15	\$10	
	215302	Discount Brokerage Services	\$22.50	\$15	
	215303	Automated Teller Machines	\$22.50	\$15	
	215304	Wholesale Wire Payments Systems	\$22.50	\$15	
	215300	Complete Risk Assessments Series (includes all four above named publications & binder)	\$67.50	\$45	
<b>GRAND TOTAL</b>					

(PLEASE PRINT)

Name \_\_\_\_\_  
 Title \_\_\_\_\_ Bank \_\_\_\_\_  
 Street Address \_\_\_\_\_  
 City \_\_\_\_\_ State \_\_\_\_\_ Zip \_\_\_\_\_  
 Signature \_\_\_\_\_

8491-5-77-077-01

176

Please place this and your check in an envelope  
and mail to this address:  
American Bankers Association  
Order Processing Dept.  
44-B Industrial Park Dr.  
Waldorf, MD 20601

Please place this and your check in an envelope  
and mail to this address:  
American Bankers Association  
Order Processing Dept.  
44-B Industrial Park Dr.  
Waldorf, MD 20601

## REQUEST FOR INFORMATION FROM PROSPECTIVE MCC/MSTC APPLICANT

\_\_\_\_\_  
*Name of Applicant Organization*

\_\_\_\_\_  
*Date*

\_\_\_\_\_  
*Contact Person / Operations or Compliance*

\_\_\_\_\_  
*Phone Number*

In response to your organization's request for participation with the Midwest Clearing Corporation/Midwest Securities Trust Company, we request that you supply us with the information identified in the attached questionnaire at your earliest convenience. In addition, copies of the following document materials (where applicable) must be submitted by MCC/MSTC applicants prior to being considered for participation.

- ✓ Current and Amended copied of FORM BD on file with SEC and DEA
- ✓ Current U-4's for Stockholders, Partners, and Officers
- ✓ Partnership Agreements or Articles of Incorporation and Amended By-Laws
- ✓ Most recent copy of "Confidential" C.P.A. Audit Report
- ✓ FOCUS I and FOCUS II Reports, for the previous twelve month period

If accepted as a MCC/MSTC participant, MSE would require the same financial reporting requirements as specified by your organization's Designated Examining Authority.

*NASD Applicants Please Note:* Part of our application review process requires that we contact your Designated Examining Authority for information regarding your regulatory and financial history. Applicants are required to grant permission in writing to their respective NASD District Office releasing pertinent information to the MCC/MSTC and its duly authorized representative. A copy of that written permission must be forwarded to the undersigned before your application can be processed.

### *Bank, Savings and Loan Association, and Trust Company Applicants*

Copies of the following document materials (where applicable) must be submitted by bank, Savings and Loan Association, and Trust Company applicants prior to being considered as a participant:

- ✓ Reports of Condition (Call Reports) for the last four quarters
- ✓ Reports of Income (Income and Dividend Reports) for the past year
- ✓ Annual audited financial statements (Form Y-6) for the past two years

If accepted as a participant, MCC/MSTC requires you to file the above reports as prescribed by your organization's Federal and State Bank or Savings and Loan regulators on a regular basis.

Request for Information from Prospective MCC/MSTC Applicant  
Page 2

Upon receipt and review of the required information, it may be determined that an on-site examination of your organization's books, records, and procedures will be necessary. Generally, the review procedure, without the on-site examination, may take fifteen (15) business days. You will be advised if and when an on-site exam will be conducted.

**If you have any questions or need any assistance, you can direct your inquiries to Paul Smith at 312-663-2723**

