FEDERAL RESERVE press release

For immediate release November 10, 1999

The Federal Reserve Board today announced its approval of the proposal by Bayerische Hypo- und Vereinsbank AG, Munich, Germany; Deutsche Bank AG, Frankfurt, Germany; and Stichting Prioriteit ABN AMRO Holding, Stichting Administratiekantoor ABN AMRO Holding, ABN AMRO Holding N.V., and ABN AMRO Bank N.V., all of Amsterdam, The Netherlands; each to retain up to 12.5 percent of the voting interests of Identrus, LLC, New York, New York, and to engage in acting as a certification authority in connection with financial and nonfinancial transactions and other related activities.

Attached is the Board's Order relating to this action.

Attachment

FEDERAL RESERVE SYSTEM

Bayerische Hypo- und Vereinsbank AG
Munich, Germany

Deutsche Bank AG
Frankfurt, Germany

Stichting Prioriteit ABN AMRO Holding
Stichting Administratiekantoor ABN AMRO Holding
ABN AMRO Holding N.V.
ABN AMRO Bank N.V.
All of Amsterdam, The Netherlands

Order Approving Notices to Engage in Nonbanking Activities

Bayerische Hypo- und Vereinsbank AG ("BHV"), a foreign banking organization subject to the Bank Holding Company Act ("BHC Act"), and Deutsche Bank AG ("Deutsche Bank") and Stichting Prioriteit ABN AMRO Holding ("ABN AMRO"), Stichting Administratiekantoor ABN AMRO Holding, ABN AMRO Holding N.V., and ABN AMRO Bank N.V., bank holding companies within the meaning of the BHC Act, have requested the Board's approval under section 4(c)(8) of the BHC Act (12 U.S.C. § 1843(c)(8)) and section 225.24 of the Board's Regulation Y (12 C.F.R. 225.24) to retain up to 12.5 percent of the voting interests in Identrus, LLC, New York, New York ("Identrus"), and to engage through Identrus and other nonbank subsidiaries in acting as a certification authority ("CA")

in the United States in connection with financial and nonfinancial transactions and other related activities.[1]

Notice of the proposal, affording interested persons an opportunity to submit comments, has been published (64 Federal Register 22,866 (1999)). The time for filing comments has expired, and the Board has considered the proposal and all comments received in light of the factors set forth in section 4(c)(8) of the BHC Act.

BHV, with total consolidated assets of $575 billion,[2] is the second largest commercial banking organization in Germany, and operates branches in New York, New York, and Chicago, Illinois, and an agency in Los Angeles, California.

Deutsche Bank, with total consolidated assets of $724 billion, is the largest commercial banking organization in Germany. Deutsche Bank controls three subsidiary banks in the United States, and operates a branch in New York, New York, and a representative office in San Francisco, California.

ABN AMRO, with total consolidated assets of $544 billion, is the

---

[1] BHV, Deutsche Bank, and ABN AMRO and its subsidiaries listed above are hereafter collectively referred to as "Notificants". Foreign banks, such as Notificants, may engage in permissible banking activities in the United States directly through a U.S. branch or agency. A foreign bank must, however, receive the Board's prior approval under section 4(c)(8) to engage in the United States through a nonbank subsidiary in activities that are closely related to banking. In this case, Notificants have requested approval under section 4(c)(8) of the BHC Act to engage in the proposed activities in the United States through Identrus and other nonbank subsidiaries to provide themselves maximum flexibility in structuring their Identrus-related activities. For purposes of this order, references to activities conducted by Notificants are intended to refer to activities conducted through Identrus or other U.S. nonbanking companies.

[2] Asset data are as of June 30, 1999, and ranking data are as of December 31, 1998.

largest commercial banking organization in The Netherlands. ABN AMRO controls seven depository institutions in Illinois and one commercial bank in New York. ABN AMRO Bank N.V. also operates branches in Boston, Massachusetts; Chicago, Illinois; New York, New York; Pittsburgh, Pennsylvania; and Seattle, Washington; and agencies in Atlanta, Georgia; Miami, Florida; Houston, Texas; and Los Angeles and San Francisco, California.

Each Notificant also engages in a number of nonbanking activities in the United States.

Proposed Activities

Identrus is a joint venture among Notificants and other commercial banks and foreign banking organizations.[3] Under the proposal, Identrus would act as the global rulemaking and coordinating body for a network of financial institutions that would act as CAs and thereby provide services designed to verify or authenticate the identity of customers conducting financial and nonfinancial transactions over the Internet and other "open" electronic networks. To provide these services, Identrus and its network of participating financial institutions (the "Identrus System") would utilize digital certificates and digital signatures created through the use of public key cryptography.

In a CA system using public key cryptography, a company generates (or is assigned) a public key/private key pair and registers as the unique "owner" of the key pair with a CA.[4] Private keys and public keys are a set of different but related mathematical functions that can be used to encrypt and decrypt electronic communications. A message encrypted by a particular private key can be decrypted

---

[3] Bank of America NT & SA, Charlotte, North Carolina, and Citibank, N.A., New York, New York, have applications pending before the Office of the Comptroller of the Currency to invest indirectly in Identrus. The Chase Manhattan Bank, New York, New York, received the approval of the New York State Banking Department to invest indirectly in Identrus. See Letter from P. Vincent Conlon, Deputy Superintendent of Banks, New York State Banking Department, to Ronald C. Mayer, The Chase Manhattan Bank, dated April 9, 1999 ("Chase Letter"). Identrus expects other U.S. commercial banks and foreign banking organizations to seek approval from appropriate regulatory authorities to invest in Identrus and engage in related activities.

[4] A number of nonbanking companies currently operate CA systems that rely on public key cryptography and provide identity authentication services to senders and receivers of electronic communications.

only by its corresponding public key. Although a private key and its corresponding public key are related, a private key cannot feasibly be derived from its corresponding public key. Thus, while a private key must be kept confidential by the company that is the registered "owner" of the key pair, the company's public key can be made publicly available without jeopardizing the confidentiality of the company's private key.

A company sending a business communication (e.g., a purchase order) over an open electronic network like the Internet to another entity uses its confidential private key to digitally sign the message being sent. A digital signature is a compressed and encrypted version of the message to which it is attached. The entity receiving the digitally signed message then uses the sender's public key to decrypt the digital signature.[5] If the receiver successfully decodes the signature with the sender's public key, the receiver can be assured that the message was created using the sender's private key.[6]

To be assured that the message was actually sent by the purported sender, however, the receiver must confirm that the private key/public key pair used to sign and decode the message is uniquely "owned" by the purported sender. A CA provides this assurance by issuing "digital certificates" certifying that the

---

[5] The sender's public key may be attached to the digitally signed communication, or the receiver of the message may obtain the sender's public key from a publicly available database.

[6] The receiver also can confirm that the message was not altered after it was signed by comparing the message received to the decrypted version of the message text embedded in the digital signature.

relevant private key/public key pair is uniquely associated with the message sender and verifying upon request the validity of such digital certificates.

Notificants and other financial institutions participating in the Identrus System ("Participants")[7] would create unique private key/public key pairs for, and issue digital certificates on behalf of, eligible customers that contract with a Participant to receive Identrus identity authentication services.[8] Each Participant would act as a repository for the digital certificates that it has issued, i.e., it would maintain a database containing information on the status of the outstanding, expired, or revoked digital certificates that it has issued to customers. Participants also would verify for third parties the validity of digital certificates issued to their customers and, upon request of the third party, may provide an explicit warranty as to the validity of the customers' digital certificates.[9] Participants also may process and transmit

---

[7] Participation in the Identrus System is available only to organizations that are engaged primarily in the business of providing financial services, are subject to regulation and examination by a government authority in their home country, and that meet certain eligibility criteria, such as minimum capital requirements and debt rating criteria. A Participant also must agree to be bound by the Identrus operating rules and execute certain participation agreements. Financial institutions would not be required to purchase an ownership interest in Identrus to become a Participant.

[8] Participants may provide Identrus-related services only to customers that have agreed to be bound by applicable provisions of the Identrus operating rules and have signed the appropriate customer agreements. The Identrus operating rules allow Participants to provide Identrus-related services only to business entities, such as corporations, and governmental organizations, and not to natural persons. The Identrus operating rules and customer agreements would make each customer contractually responsible for ensuring that its private key is kept confidential.

[9] The operating rules of the Identrus System would provide that a company relying on a digital certificate issued by a Participant would have recourse against the Participant only if the company purchased an explicit warranty from the Participant

(continued...)

verification and warranty requests received from customers concerning digital certificates issued by other Participants in the Identrus System. In addition, Participants may provide customers with a limited range of software and hardware required for customers to utilize the Identrus System.[10]

Identrus would provide the infrastructure framework within which Participants would act as CAs and provide related services. The primary function of Identrus would be to act as the "root certification authority" of the Identrus System, i.e., issuing digital certificates to Participants that establish the status of Participants as CAs in the Identrus System and authenticating for customers of, and Participants in, the Identrus System the identity of Participants.[11] Identrus also would (i) establish and maintain the operating rules governing the Identrus System, including the minimum technical requirements for digital certificates and other components of the System; (ii) monitor compliance by Participants with the System's operating rules

---

(...continued)
and then only up to amount of the purchased warranty. A Participant that issues a digital certificate could refuse to issue a warranty with respect to a digital certificate for any *bona fide* reason. The Identrus System would limit the aggregate amount of warranties that a Participant may have outstanding at any one time and would require each Participant to post collateral with Identrus to cover its warranty exposure.

[10] For example, Participants may provide smart cards containing digital certificates and smart card readers to their customers.

[11] Digital certificates issued by a Participant to a customer are digitally signed by the Participant with the Participant's own private key and are accompanied by a digital certificate issued by Identrus. The digital certificates issued by Identrus would certify that the Participant is an authorized Participant in the Identrus System and that the private key used by a Participant to digitally sign its certificates is uniquely associated with the Participant, thereby authenticating the identity of the Participant.

and technical standards; and (iii) monitor collateral requirements and aggregate warranty exposure for Participants in the Identrus System.[12]

Permissibility of Proposed Activities

Section 4(c)(8) of the BHC Act provides that a bank holding company may, with the Board's approval, engage in any activity that the Board determines to be closely related to banking.[13] The Board previously has authorized bank holding companies under section 4(c)(8) of the BHC Act to act as CAs and provide identity authentication services in connection with payment-related and other financial transactions conducted over electronic networks.[14] The Board has not previously authorized bank holding companies under section 4(c)(8) to act as CAs or provide identity authentication services in connection with nonfinancial transactions.

In determining whether an activity is closely related to banking, the Board and the courts look to whether (1) banks generally provide the proposed services; (2) banks generally provide services that are operationally or functionally so similar to the proposed services as to equip them particularly well to provide the proposed services; or (3) banks generally provide services that are so integrally related to the

---

[12] The activities of Notificants and Identrus would be limited to providing the identity authentication and related services described above. Notificants and Identrus would not provide a general encryption or electronic message service, or any warranty of the underlying financial or nonfinancial transaction between customers whose identities are authenticated through the use of the Identrus System.

[13] 12 U.S.C. § 1843(c)(8).

[14] See 12 C.F.R. 225.28(b)(14); Banc One Corporation, Inc., 83 Federal Reserve Bulletin 602, 606 (1997); Citicorp, 68 Federal Reserve Bulletin 505, 510 (1982).

proposed services as to require their provision in a specialized form.[15]

Banks and bank holding companies have long provided identity authentication services in connection with nonfinancial transactions conducted by third parties and their own traditional banking and lending activities. For example, banks and bank holding companies are authorized to provide notary services to customers.[16] The role of a notary is to authenticate signatures on financial or nonfinancial documents for the benefit of third parties.[17] In order to verify a signature on a paper-based document, a notary must verify the identity of the person signing the document. The role served by a CA with respect to electronic documents is functionally similar to the role served by a notary with respect to paper-based documents.[18]

Similarly, banks traditionally have identified their customers to third parties through the issuance of letters of introduction or letters of reference.[19] In addition, banks

---

[15] See National Courier Association v. Board of Governors of the Federal Reserve System, 516 F.2d 1229, 1237 (D.C. Cir. 1975). In addition, the Board may consider any other basis that demonstrates that the proposed activity has a reasonable or close connection or relationship to banking or managing or controlling banks. See Board Statement Regarding Regulation Y, 49 Federal Register 806 (1984); Securities Industry Association v. Board of Governors of the Federal Reserve System, 468 U.S. 207, 210-11 n.5 (1984).

[16] See OCC Unpublished Interpretive Letter dated June 11, 1985; Popular, Inc., 84 Federal Reserve Bulletin 481 (1998).

[17] 58 Am. Jur. 2d Notaries Public § 31 (2d ed. 1989).

[18] The American Bar Association, for example, has noted that the issuance of digital certificates by CAs is "analogous to traditional certification processes undertaken by notaries with respect to documents executed with pen and ink." See Digital Signature Guidelines, Information Security Committee, Electronic Commerce and Information Technology Division, Section of Science and Technology, American Bar Association, p. 54 (Aug. 1, 1996).

[19] Banks have drafted letters of introduction or letters of reference on behalf of their

(continued...)

and bank holding companies routinely authenticate the identity of customers and noncustomers in connection with their authorized check cashing functions.[20] Banks and bank holding companies also have long been authorized to issue signature guarantees to issuers of securities and their transfer agents in connection with the transfer of securities.[21] A bank issuing a signature guarantee warrants that the signature of the customer indorsing a certificated security or authorizing the transfer of an uncertificated security is authentic. The issuing bank also warrants that the signer was an appropriate person to indorse the security or authorization (or, if the signature is by an agent, that the agent had actual authority to act on behalf of the appropriate person) and the signer had legal capacity to sign.[22] In light of these

---

(...continued)
customers that serve the purpose of introducing the customer to other banks or third parties with which the customer seeks to do business. See McLeod v. Fourth National Bank of St. Louis, 122 U.S. 528, 534 (1887); OCC Interpretive Letter No. 610, reprinted in [1992-1993 Transfer Binder] CCH Fed. Banking L. Rep. ¶ 83,448 (Oct. 8, 1992).

[20] Under the Uniform Commercial Code, a bank that accepts a check for deposit warrants to the drawee bank that all indorsements on the check are genuine, and the bank is liable to the drawee bank for the amount of the check plus expenses and lost interest if an indorsement on the check was forged. See, e.g., N.Y. U.C.C. § 4-207 (McKinney 1991).

[21] See Letter from William B. Glidden, OCC Assistant Director, dated Dec. 5, 1985; see also Acceptance of Signature Guarantees from Eligible Guarantor Institutions, Exchange Act Rel. No. 29,663, [1983-1984 Transfer Binder] Fed. Sec. L. Rep. (CCH) ¶ 84,825, at 82,119 (Sept. 9, 1991); U.S. League of Savings Associations, SEC No-Action Letter, [1982-1983 Transfer Binder] Fed. Sec. L. Rep. (CCH) ¶ 77,412, at 78,500 (Apr. 29, 1983). Broker-dealer subsidiaries of bank holding companies also have provided signature guarantees.

[22] See, e.g., N.Y. U.C.C. § 8-306(a) and (b) (McKinney 1999).

warranties, a bank providing a signature guarantee must verify the identity of the customer providing the indorsement or signing the instruction.[23]

Furthermore, identity authentication services are an integral part of many traditional banking functions. Accordingly, banks and bank holding companies have developed sophisticated methods for authenticating the identity of customers and noncustomers that transact business or communicate with the bank or bank holding company through electronic means or otherwise. Many of these activities are operationally and functionally similar to the proposed activities and equip banks and bank holding companies particularly well to provide the proposed services. For example, banks and bank holding companies maintain systems to electronically authenticate the identity of persons engaged in credit and debit card, automated teller machine ("ATM"), home banking, and wire transfer transactions with the institution.[24] Banks and bank holding companies also electronically authenticate the identity of persons in connection with the check and credit card verification services they are authorized to provide to merchants and other businesses.[25]

---

[23] A bank issuing a signature guarantee is liable to the issuer of the security or its transfer agent for any loss that results from a breach of any of these warranties by the bank. See, e.g., N.Y. U.C.C. § 8-306(h) (McKinney 1999).

[24] Article 4A of the Uniform Commercial Code, in fact, encourages banks to develop and maintain commercially reasonable security procedures, such as algorithms or other encryption devices, for authenticating the identity of customers that transmit wire transfer instructions to the bank. See, e.g., N.Y. U.C.C. § 4-A-202 (McKinney 1999).

[25] See 12 C.F.R. 225.28(b)(2)(iii); Barnett Banks of Florida, Inc., 71 Federal Reserve Bulletin 648 (1985); OCC Unpublished Interpretive Letter dated March 26, 1982.

The Board notes, moreover, that state banks and national banks recently have been authorized to act as CAs and provide identity authentication services in connection with financial and nonfinancial transactions conducted over electronic networks.[26] Based on the foregoing, the Board concludes that acting as a CA and, more generally, authenticating the identity of customers conducting financial and nonfinancial transactions are activities that are closely related to banking within the meaning of section 4(c)(8) of the BHC Act.

As discussed above, Identrus and Notificants also propose to engage in a number of activities as part of and in connection with their proposed CA activities. These activities include (i) processing, transmitting, and storing data necessary for the operation of the Identrus System, such as digital certificates, requests for verification of digital certificates, and warranty requests; (ii) developing and marketing software and hardware necessary for the operation of the Identrus System; and (iii) complying with, monitoring, and enforcing the collateral posting requirements associated with identity warranties. In addition, Identrus would establish operating policies, procedures, and guidelines for the Identrus System. The Board's Regulation Y permits bank holding companies to provide data processing and data transmission services and facilities (including software and hardware) for the processing and transmission of financial, banking, or economic data, and to engage in activities related to making, acquiring, brokering, or servicing extensions of credit, such as posting collateral and monitoring collateral requirements.[27] Regulation Y also permits bank holding companies to engage in

---

[26] See Chase Letter; OCC Conditional Approval No. 267 (Jan. 12, 1998).

[27] See 12 C.F.R. 225.28(b)(2) and (14). Under Regulation Y, a bank holding

(continued...)

incidental activities that are necessary to the conduct of an activity that is closely related to banking.[28] Identrus and Notificants have represented that they would engage in the additional activities only in connection with their CA activities and would not engage in such activities separate or apart from their CA activities. Notificants also have committed that the data processing and data transmission activities of Notificants and Identrus, including any proposed development or sale of hardware and software, will comply with the Board's regulations and interpretations. In light of the nature of these additional activities, the fact that they would be conducted only in connection with the CA activities of Identrus and Notificants, and all other facts of record, the Board concludes that these activities are encompassed within the activities previously approved by the Board by regulation or are incidental to the permissible CA activities of Identrus and Notificants and, therefore, are permissible under Regulation Y.[29]

(...continued)
company may develop and sell hardware and software that is designed and marketed for the processing and transmission of financial, banking, or economic data, and may develop and sell general purpose hardware so long as such general purpose hardware does not constitute more than 30 percent of the cost of any packaged offering. See 12 C.F.R. 225.28(b)(14).

[28] 12 C.F.R. 225.21(a)(2).

[29] Notificants may engage in data processing and data transmission activities, including the development and sale of hardware and software, pursuant to this order only to the extent such activities are necessary to permit the proper operation of the Identrus System. Notificants and Identrus also must conduct their data processing and data transmission activities subject to the software and hardware limitations contained in Regulation Y.

Other Considerations

In order to approve the notices, the Board also must determine that the performance of the proposed activities by Notificants and Identrus "can reasonably be expected to produce benefits to the public . . . that outweigh possible adverse effects, such as undue concentration of resources, decreased or unfair competition, conflicts of interests, or unsound banking practices."[30] As part of its evaluation of these factors, the Board considers the financial and managerial resources of Notificants and their subsidiaries, and the effect the transaction would have on such resources.[31] The Board notes that each Notificant maintains capital equivalent to the capital levels that would be required of a U.S. banking organization. Based on all the facts of record, including confidential examination reports and financial information submitted by Notificants, the Board has concluded that financial and managerial considerations are consistent with approval of the proposal.

The Board has carefully considered the possibility that Identrus, Notificants, and their customers could expose themselves to the risks of electronic interception, interference, and fraud by operating and participating in a system that provides digital certification services for transactions conducted over open electronic networks like the Internet. The Board has carefully considered the proposal in light of these risks and the policies and procedures that the Identrus System would use to mitigate such risks. The Board notes that an organization would be eligible to become a Participant in the Identrus System only if it provides financial services, is regulated and examined by a government authority in its home

---

[30] 12 U.S.C. § 1843(c)(8).

[31] See 12 C.F.R. 225.26(b).

country, meets minimum capital standards, and has a minimum long-term debt rating. Identrus and Notificants also intend to use sophisticated cryptographic methods to seek to ensure the security of digital certificates and to adopt a highly secure root CA technology.

In addition, as noted above, Participants and customers would be required to enter into written contracts that carefully define the functions, responsibilities, and scope of liability of the relevant parties and require the Participant and customer to comply with the operating rules of Identrus before they are permitted to participate in the Identrus System.[32] Each digital certificate issued by a Participant would indicate that the recipient of the certificate may not rely on the certificate unless the recipient purchases a separate warranty from the Participant issuing the certificate. Furthermore, Identrus proposes to (i) establish limits on each Participant's per transaction and aggregate warranty exposure and monitor each Participant's compliance with these limits, (ii) require Participants to provide collateral to secure their warranty exposure and monitor compliance with such collateral requirements, and (iii) maintain a comprehensive auditing system that would monitor the adherence of Participants to the Identrus operating rules and technical standards. The Board recognizes that neither the cryptographic methods employed by Identrus nor any other security system can provide absolute protection against the risks noted

---

[32] Notificants have indicated that the Identrus System is in the process of finalizing its operating rules, including the technical specifications for the system, and sample Participant and customer agreements. The Board has carefully reviewed the Identrus System's draft operating rules and agreements, and Notificants have committed to provide the Federal Reserve System with the final version of the operating rules (including the technical specifications) and sample Participant and customer agreements prior to commencing operations.

above. The nature of these risks is not different, however, from those to which more traditional banking operations are exposed in other forms. The Board expects banking organizations considering whether to act as CAs to analyze carefully the associated risks, and to evaluate carefully whether those risks are consistent with their policies relating to the security of customer information and other data.[33] The Board believes that such analyses and evaluations would mitigate the risk that acting as a CA would result in unsound banking practices.[34]

The Board also has carefully considered the competitive effects of the proposal. Notificants do not currently act as CAs in the United States, and consummation of the proposal would increase competition in the market for CA services. In addition, the Board notes that the Identrus System would permit Notificants and other Participants in the Identrus System to compete with each other to provide CA and related services to customers.

Notificants have stated that consummation of the proposal would facilitate the use of

---

[33] The Board notes that Identrus has engaged an independent public accounting firm to conduct a detailed risk analysis of the Identrus System. Moreover, Notificants have agreed to treat Identrus as a subsidiary for purposes of the BHC Act, and Identrus has committed to include a provision in any contract with a vendor that provides services covered by the Bank Service Company Act (12 U.S.C. § 1861 et seq.) indicating that the Identrus-related operations of that vendor will be subject to the examination and regulatory authority of the Board.

[34] Notificants have committed that neither Notificants nor Identrus will represent that the Board's approval of these notices constitutes an endorsement of Notificants' or Identrus's products or services by the Federal Reserve System, and neither Notificants nor Identrus will indicate in any of their marketing efforts or materials, either oral or written, that the Federal Reserve System assures or has approved or endorsed the security, functionality, or effectiveness of the products or services offered by Notificants or Identrus.

the Internet and other open electronic networks for business-to-business electronic commerce, and allow companies to reduce the transaction costs associated with doing business. The Board also believes that consummation of the proposal would enhance the ability of Notificants to meet the needs of their customers. In addition, as the Board previously has noted, there are public benefits to be derived from permitting capital markets to operate so that banking organizations can make potentially profitable investments in nonbanking companies and from permitting banking organizations to allocate their resources in the manner they consider to be most efficient when such investments and actions are consistent, as in this case, with the relevant considerations under the BHC Act.[35]

Based on the foregoing and all other facts of record, the Board has determined that consummation of the proposal can reasonably be expected to produce benefits to the public that outweigh any potential adverse effects of the proposal. Accordingly, based on all the facts of record, the Board has determined that the balance of public interest factors that the Board must consider under the proper incident to banking standard of section 4(c)(8) of the BHC Act is favorable and consistent with approval.

---

[35] See, e.g., Banc One Corporation, 84 Federal Reserve Bulletin 553 (1998).

Conclusion

Based on the foregoing and all the facts of record, the Board has determined that the proposal should be, and hereby is, approved. The Board's approval is specifically conditioned on compliance by Notificants with all the commitments made in connection with the notices, including the commitments discussed in this order, and the conditions set forth in this order. The Board's determination also is subject to all the conditions set forth in Regulation Y, including those in sections 225.7 and 225.25(c) of Regulation Y (12 C.F.R. 225.7 and 225.25(c)), and to the Board's authority to require such modification or termination of the activities of a bank holding company or any of its subsidiaries as the Board finds necessary to ensure compliance with, or to prevent evasion of, the provisions of the BHC Act and the Board's regulations and orders issued thereunder. These commitments and conditions are deemed to be conditions imposed in writing by the Board in connection with its findings and decision, and, as such, may be enforced in proceedings under applicable law.

This proposal shall not be consummated later than three months after the effective date of this order, unless such period is extended for good cause by the Board or by the appropriate Federal Reserve Bank, acting pursuant to delegated authority.

By order of the Board of Governors,[36] effective November 10, 1999.

(signed)

---

[36] Voting for this action: Chairman Greenspan, Vice Chairman Ferguson, and Governors Kelley, Meyer, and Gramlich.

Robert deV. Frierson
Associate Secretary of the Board