



OCC ADVISORY LETTER

Comptroller of the Currency
Administrator of National Banks

Subject: Internet-Initiated ACH
Debits/ACH Risks

TO: Chief Executive Officers of All National Banks, Service Providers and Software Vendors, Department and Division Heads, and All Examining Personnel

PURPOSE

This advisory alerts national bank management and boards of directors to specific Automated Clearing House (ACH) risks and emphasizes the importance of sound ACH risk management practices. In particular, this advisory describes a recently approved amendment to the operating rules of the National Automated Clearing House Association (NACHA). The amendment is designed to enhance security for ACH debits initiated through the Internet and mandates the use of security measures that meet minimum standards. National banks that transmit certain Internet-initiated ACH debits will be deemed to warrant that their customers who originate the entries have met these standards. The banks can be held liable for losses that result from a failure of their customers to meet these standards. In order to fulfill their responsibilities, management and boards of directors of national banks must understand the nature of ACH risks, ensure the bank has procedures in place to comply with the NACHA operating rules, and ensure appropriate risk controls exist within the bank.

BACKGROUND

The ACH network through which electronic payments are distributed and settled has existed since the early 1970s. ACH debit entries transfer funds from another party (receiver) to the originator of the entry (originator). For example, for a mortgage payment made through ACH debit, the receiver is the mortgage payor and the originator is the mortgage creditor. On the other hand, ACH credit entries transfer funds from the originator to the receiver. For example, for employee payroll distributions made through ACH credit, the employer is the originator and the employees are the receivers.

As the industry develops new and innovative uses for ACH, and as both ACH activity and the number of participants in the network (including third parties)¹ grow, the Office of the Comptroller of the Currency (OCC) believes that there is an increased need for ACH risk management. The volume and dollar amount of ACH originations have been increasing significantly and in particular with regard to transactions initiated through the Internet.

¹ See NACHA Operations Bulletin (June 2, 2000) discussing the risks involved with third-party direct access to the ACH Network and with Internet-initiated ACH payments at http://www.nacha.org/ACHNetwork/2000_bulletins___2.doc.

DISCUSSION

As with other electronic payment mechanisms, there are inherent risks in using the ACH, most notably strategic, reputation, transaction, credit, and compliance risk. Federal banking agencies have encouraged sound ACH risk management practices for a number of years.² The risks are particularly acute concerning ACH entries initiated through the Internet in light of the anonymity of that medium and the volume and velocity of transactions that can be originated. The recently approved amendment to NACHA's operating rules with respect to Internet-initiated payments³ presents management and boards of directors with new challenges. The amendment, effective on March 16, 2001, is designed to enhance security for ACH debits initiated through the Internet. It increases the warranties that accompany the transmission of certain Internet-initiated ACH entries by an originating depository financial institution (ODFI) to a receiver's account with a receiving depository financial institution (RDFI).

Management and boards of directors should review the amendment with legal counsel. In addition, management should review agreements with originators and third parties, including clauses that may provide for indemnification of the bank, in light of the new warranty liability imposed on ODFIs by the amendment and described below.

The most important changes introduced by the amendment are as follows:

- A new Standard Entry Class (SEC) Code, WEB, has been created to uniquely identify a debit entry initiated pursuant to an authorization obtained through the Internet to effect a transfer of funds from a consumer account. WEB entries will be further identified as either recurring entries or nonrecurring entries;⁴
- Originators of WEB entries (*e.g.*, merchant customers of national banks) are required to
 - Employ commercially reasonable⁵ fraudulent-transaction detection systems to screen the entries in order to minimize the risk of fraud related to Internet-initiated payments.⁶
 - Use commercially reasonable procedures to verify that routing numbers are valid.
 - Establish a secure Internet session with each receiver prior to the key entry by the receiver of any banking information. Originators are required to use a commercially reasonable security technology providing a level of security that, at a minimum, is equivalent to 128-bit encryption technology.

² See, *e.g.*, FFIEC Information Systems Examination Handbook, chapter 21 (1996).

³ Banks may purchase from the NACHA a copy of the 2001 operating rules incorporating the amendment. Purchase requests may be made at <http://www.nacha.org> or at (703) 561-1100.

⁴ The amendment does not impose additional requirements on RDFIs. We note, however, that the new SEC Code permits RDFIs to identify Internet-initiated entries for appropriate treatment.

⁵ Banks should refer to NACHA guidance on the "commercially reasonable" standard.

⁶ Originators' authentication of receivers is critical to decreasing the risk of fraud.

- Conduct an annual audit to ensure that the financial information obtained from receivers is protected by security practices and procedures that include, at a minimum, adequate levels of (1) physical security to protect against theft, tampering, or damage; (2) personnel and access controls to protect against unauthorized access and use; and (3) network security to ensure capture, storage, and distribution of financial information. The first audit must be completed by December 31, 2001.
- ODFIs are required⁷ to
 - Ensure that originators are in compliance with the above requirements on a continuing basis. Under the amendment, ODFIs that transmit WEB entries warrant that originators have conformed to those new requirements.
 - Conform with an additional warranty, in the case of a WEB entry initiated by an originator that is not a natural person, that the ODFI has
 - Used a commercially reasonable method to establish the identity of the originator;
 - Established procedures to monitor the creditworthiness of the originator on an ongoing basis;
 - Established an exposure limit for the originator and implemented procedures to review that exposure limit periodically;
 - Implemented procedures to monitor entries initiated by the originator relative to its exposure limit across multiple settlement dates.

SUMMARY

The OCC recognizes that ACH-related products and services provide national banks an opportunity to retain customers and attract new business. ACH transactions, especially Internet-initiated transactions, present important risk management and legal liability challenges to management and boards of directors. OCC examiners will continue to assess whether ACH risk management practices are commensurate with ACH activities and risks and conform to the NACHA operating rules. As the ACH network develops further, the OCC may provide further guidance on ACH-related risks and controls.

⁷ The annual audit requirement under the NACHA operating rules has also been amended to include verification that the ODFI is meeting these new requirements.

Questions concerning this advisory may be directed to the OCC's Core Policy unit at (202) 874-5490.

Mark L. O'Dell
Deputy Comptroller
Core Policy