

NR 98-88
August 26, 1998

OCC Issues Guidance for Sound Management of PC Banking
Risks

WASHINGTON, D.C. -- The Office of the Comptroller of the Currency issued a bulletin today providing guidance to banks on ways to control risk arising from the use of personal computers in retail banking. The OCC estimates that nearly a quarter of the nation's 2,600 national banks engage in some form of PC banking.

The guidance, which provides additional detail on issues highlighted in an OCC technology risk management bulletin issued in February, recognizes that banks can achieve competitive advantages and realize new business opportunities by offering on-line services to consumers. However, the bulletin also outlines various risks in PC banking and offers sound controls that, if properly implemented and practiced by national banks, can help to manage these risks.

"PC banking provides enormous opportunities for banks," said Acting Comptroller Julie L. Williams. "But the online environment gives rise to a new set of risks which banks must learn to manage effectively if they are to maintain customer confidence and assure the development of safe and sound electronic banking systems."

The most common source of risk in PC banking arises from on-line transactions, particularly if conducted over the Internet. Risks range from the possibility of unauthorized intrusions and data alteration to system failures and computer viruses. National banks need to implement risk management practices that establish adequate policies and procedures, internal controls and system monitoring. In addition to transaction risk, today's guidance also addresses strategic, compliance and reputation risks.

The guidance also encourages security policies, awareness and controls that should result in reliable access control, user authentication, data integrity, data privacy, and transaction verification. In addition, the guidance encourages banks to test system "firewalls" and security controls by attempting to penetrate the system from the outside at least once a year.

National banks that out-source their PC banking systems to service providers have less "hands-on" involvement in detecting unauthorized intrusions into their systems. Smaller banks in particular are more likely to out-source PC banking services. National banks need internal processes to manage these third parties, including the ability to review their financial condition, to stay informed of their internal control practices, to establish rights in the event a third party fails, and to set conditions for terminating or changing service providers without incurring substantial liability.

National banks are advised that laws and regulations which apply to online activity may change over time to accommodate new developments in electronic banking. Banks should monitor developments at state and federal levels and consult legal counsel to ensure appropriate interpretation and implementation of changed rules and regulations.

Today's bulletin will be followed later this year by guidance on risks in electronic authentication, including digital signatures and certification activities.

#

The OCC charters, regulates and examines approximately 2,600 national banks and 66 federal branches and agencies of foreign banks in the United States, accounting for 58 percent of the nation's banking assets. Its mission is to ensure a safe, sound and competitive national banking system that supports the citizens, communities and economy of the United States.