NR 98-86
August 20, 1998

OCC Warns Banks About "Pretext Calling" by Information Brokers

WASHINGTON, D.C. -- The Office of the Comptroller of the Currency today warned national banks to take precautions against a growing threat to the confidentiality of customer account information. In an advisory letter to the banks, the agency described how confidential information may be gathered illicitly from banks and other businesses by persons pretending to be a particular customer -- the practice of "pretext calling."

"Banks need to be on their guard against this invasion of their customers' privacy," said acting Comptroller of the Currency Julie L. Williams. "We expect them to take steps to protect themselves and their customers from the unscrupulous acts of some information brokers."

The advisory was jointly prepared by the OCC, the FDIC, the Office of Thrift Supervision, the Federal Reserve Board, the Secret Service, the Federal Bureau of Investigation, the Internal Revenue Service and the Postal Inspection Service, and is expected to be issued shortly by the other federal banking agencies.

The guidance advises institutions that they should, at a minimum, establish guidelines setting forth precisely what types of information can be disseminated over the phone and under what circumstances.

As part of their internal controls, banks should consider adopting policies that prohibit disclosure of account information over the phone unless the caller provides an authorization code, similar to the personal identification number depositors use to access accounts through automated teller machines. The code should not be one that is easily associated with the customer, such as a mother's maiden name or the person's social security number. Alternatively, banks could use caller identification services to verify that the caller is phoning from the telephone number listed in the account record.

In addition, the advisory suggests that bank security or audit departments test their institutions by periodically calling (or using third parties to call) various departments and attempting to obtain account information about individual customers. Any weaknesses detected should be addressed through enhanced training, procedures and controls.

The OCC also reminded national banks that customer confidentiality can be compromised through other means, including burglary, unauthorized access to an institution's computer systems or bribery of employees. Banks are expected to have effective procedures in place to limit access to confidential information on a need-to-know basis, and to safeguard data. For example, sensitive documents should be properly disposed of and

computer systems should be secure.

The advisory notes that efforts to obtain customer account information surreptitiously could violate state or federal laws prohibiting unfair or deceptive practices, as well as the federal wire fraud statute. Institutions that release account information to brokers may be in violation of state privacy laws.

Institutions should notify the proper authorities if they believe someone has illicitly attempted to obtain confidential account data. A Suspicious Activity Report should be filed with Treasury's Financial Crimes Enforcement Network, and the institution's primary federal bank regulator, as well as the Federal Trade Commission and the appropriate state agency, should be contacted. The appropriate law enforcement agency should be contacted if a fraud requiring immediate attention is suspected.

# # #

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