ALERT 2000–1

OCC ALERT

Comptroller of the Currency
Administrator of National Banks

Subject: Internet Security: Distributed Denial of Service Attacks

TO: Chief Executive Officers and Chief Information Technology Officers of National Banks, Federal Branches, Service Providers and Software Vendors; Department and Division Heads, and Examining Personnel

In recent days, many high profile Internet-based electronic commerce Web sites have been victims of attacks. The attacks have interrupted customer access to Internet Web sites by flooding these targeted sites with more information than their computers can handle. This flooding of information may force the Web site to suspend normal service, and is commonly referred to as a "distributed denial of service" attack (DDoS). DDoS attacks represent a new and significant threat to Internet Web site availability and merit close scrutiny by management.

Many computer security experts believe these attacks may be perpetrated by commandeering computer servers of unknowing parties (*e.g.*, companies, government agencies, universities) in a concerted effort to flood targeted Web sites. To ensure that your institution is not an unwitting participant in these attacks, you should check your own computer systems. For additional information on how to prepare for DDoS attacks, Carnegie Mellon University's CERT/CC provides helpful information and can be accessed through the Internet at the following address: http://www.cert.org/reports/dsit_workshop.pdf

Institutions should review and update their capacity for responding to these attacks and other emerging information security threats. Institutions should periodically test network security; update risk assessment techniques, risk mitigation controls, and policies and procedures (as outlined in other OCC and Federal Financial Institution Examination Council guidance); and consider participating in information-sharing organizations (*e.g.*, Financial Services Information Sharing and Analysis Center, Carnegie Mellon University's CERT/CC, Federal Bureau of Investigation's Infragard program). In addition, contingency plans should be current. Institutions should be prepared, as part of the contingency planning process, to reassure the public that the temporary malfunction of their Web sites does not jeopardize their funds and that the bank is fully capable of meeting their banking needs through other delivery channels.

In the event that your institutions is a victim of a DDoS attack or adversely affected by such an attack, you should report this information to law enforcement authorities, file a Suspicious Activity Report (SAR), and notify your OCC examiner.

Questions regarding this alert should be directed to Clifford A. Wilke, Director, Bank Technology Division at (202) 874-5920 or via E-mail: clifford.wilke@occ.treas.gov.

_____

Clifford A. Wilke
Director, Bank Technology Division