ALERT 2000–9

OCC ALERT

Comptroller of the Currency
Administrator of National Banks

Subject: Protecting Internet Addresses of National Banks

TO: Chief Executive Officers of All National Banks; All State Banking Authorities; Chairman, Board of Governors of the Federal Reserve System; Chairman, Federal Deposit Insurance Corporation; Chairman, National Credit Union Administration; Conference of State Bank Supervisors; All Examining Personnel; Service Providers

PURPOSE AND BACKGROUND

This alert highlights the need for banks to carefully select and protect their Internet addresses. Recently, several banks discovered Internet Web sites with Internet addresses similar to the addresses of their national bank Web sites. This confusing situation resulted in some bank customers mistakenly transmitting confidential information to these other similar Web sites.

Banks and others establish Internet addresses by registering a domain name through a domain name registration authority. Domain name registration information typically consists of the name of the registered owner, contact information, and technical information necessary to operate the domain naming system. Since domain name registration services are primarily concerned with establishing unique names, they do not impose restrictions on the registration of similar names.

A hypothetical example of a domain name is examplebank.com, which can coexist with examplebank.net and examplebank.org. Country suffixes also can be used to create similar names, (e.g., examplebank.de for Germany). Although the prefix of "www" is often used to denote a Web address (e.g., www.examplebank.com), it is possible to include "www" in a domain (e.g., www.wwwexamplebank.com). To avoid customer confusion, banks should consider the following actions in establishing and monitoring Internet addresses.

DOMAIN NAME SELECTION AND REGISTRATION

Banks should ensure their domain name is registered to them, under their control, and clearly communicated to their customers. In order to avoid customer confusion, banks should consider registering similar domain names. When another entity holds the registration to a similar domain name, banks should consider the risk of customer confusion between the two names. Where the risk of confusion is unacceptably high, the bank can take actions such as increasing customer education efforts, selecting a different domain name, or seeking to acquire the similar domain name from its owner. The bank also can dispute the use of the other domain name under the terms of the domain name license agreement. Under those terms, registered domain name owners are required to abide by the policy located at http://www.domainmagistrate.com/dispute-policy.html. In general, the dispute policy provides for a mandatory administrative proceeding

when a domain name is identical, confusing, or similar to trademarks or service marks; is registered to someone with no legal right or legitimate interest in the domain name; or is used in bad faith. For this reason, banks should consider establishing a trademark for their domain names. The bank also may be able to initiate immediate action in federal district court under the recently enacted Anticybersquatting Consumer Protection Act, 15 USC 1125 (d). In the event the similar domain name remains registered to someone other than the bank, the bank should consider surveying the domain periodically to ensure that the use of the domain does not pose an unacceptable risk to the bank or its customers.

CONTROLLING CHANGES TO DOMAIN NAME REGISTRATION

Domain name registration authorities will change registration information upon request. An unauthorized change to the bank's registration information, however, could result in the loss of a bank's on-line identity and a misdirection of its customer communications. To limit the risk of unauthorized changes, banks can select a method of communicating with their domain name registration authority that ensures an adequate degree of authentication. In addition, banks should consider establishing internal procedures to ensure that bank communications with the registration services are authorized.

PROTECTING AGAINST DOMAIN NAME SERVER INTRUSIONS

An intrusion into a domain name server can result in a bank losing its on-line identity, even if a bank carefully selects and protects its domain names. Banks should protect against domain name server intrusions using the guidance provided in the OCC Bulletin 2000-14 "Infrastructure Threats -- Intrusion Risks" (May 15, 2000).

SUSPICIOUS ACTIVITY REPORTING

Banks that become aware of identity theft or similar crimes perpetrated in conjunction with the use of similar domain names, unauthorized changes to domain name registrations, or other actions should file a Suspicious Activity Report in accordance with Regulation 12 CFR 21.11 and the instructions of the Suspicious Activity Report form.

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