FDIC

Federal Deposit Insurance Corporation

November 8, 2000

Bank Technology Bulletin

TO: Chief Executive Officers of All FDIC-Supervised Banks

SUBJECT: *Protecting Internet Domain Names*

As the number of banks with Web sites continues to grow steadily, the number of incidents involving disputes, confusion and fraud related to their Internet domain names also has increased. To protect their online identities, banks can employ internal controls that ensure timely registration and renewal of relevant domain names, periodically review the status of similar domain names, and be familiar with the formal and informal dispute resolution processes.

This bulletin alerts senior bank management to potential domain name-related problems, and highlights actions that may help to avoid or resolve such problems.

DEFINITIONS

Internet Domain Name: A unique identifier for an Internet site that can be compared to a mailing address for a physical location. A domain name often includes two or more parts separated by periods. Common suffixes (called "top-level domains") include *.com*, *.net* and *.org*, in addition to country-related domains such as *.us* for the United States. Separate registration is required for ownership of each variation of a domain name (e.g., *bankname.com*, *bankname.net* and *bankname.org).*

Cybersquatting (Cyberpiracy): The act of registering a particular Internet address – usually a well-known company name – with the intent of holding it until it can be sold for profit.

DOMAIN NAME REGISTRATION

The process for registering a domain name is relatively fast and simple. Applicants submit a request to one of several registrars indicating the desired domain name, the name of the owner, contact information, and details about the computers that will support the domain name service. The registration and payment process can be completed online. Any domain name can be registered, provided that it not currently registered to someone else. This process does not preclude the granting of similar names to separate parties.

Nature of the Problem

Internet domain names have been used to perpetrate fraud and have led to both public confusion and legal disputes. For example, fraudulent operators have created Web sites that attempt to mislead customers into disclosing their passwords or other sensitive information. They do this by acquiring domain names that may be similar in spelling to those of legitimate Web sites. Some Web sites also have been created to publish harmful information about an organization, using a domain name that is similar to the "target." Another problem involves "cybersquatters" who have attempted to sell desirable domain names to companies at exorbitant prices. These situations could result in considerable reputational harm and financial cost.

Risk Management Techniques

To prevent customer confusion, reputational harm, fraud and legal disputes, bank management can employ a number of practices and techniques. Timely registration and renewal of a bank's domain name(s) are important to assure that the bank acquires and retains ownership of the Internet addresses that it desires. Any lapses in registration could result in the loss of a domain name to another party.

Bank management may choose to consider acquiring more than one domain name to retain control over the use of all similar names. However, this strategy may entail financial and administrative costs. Either way,

institutions may benefit from conducting periodic Internet searches to determine whether there are names being used that are similar to their domain name, legal name or other trade/product names. In addition to similar domain names that have different suffixes (e.g., *bankname.com* and *bankname.net*), management also may want to look for variations in spelling and punctuation (e.g., *bankname.com* and *bank-name.com*).

Possible Resolutions

Depending on the nature of the problem involving a bank's domain name, management may pursue various courses of action. Legal recourse may be available under the Anti-Cybersquatting Consumer Protection Act, 15 U.S.C. §1125(d), which prohibits registering or using a domain name that is confusingly similar to another name, with the intent to profit. Other situations involving Web sites that are used to promote fraud or illegal activity can be addressed under existing laws that address financial fraud and computer crime (e.g., 18 U.S.C. §1101 - Fraud and False Statements, 18 U.S.C. §1030 - Fraud in Connection with Computers, 18 U.S.C. §1343 - Wire Fraud). Banks also are reminded that suspicious activity involving domain names should be reported according to existing instructions for filing Suspicious Activity Reports with their primary federal regulator and law enforcement agencies.

Disputes over domain names also can be handled by private arbitrators. A dispute resolution process, outlined in the Uniform Domain-Name Dispute-Resolution Policy, has been established by the Internet Corporation for Assigned Names and Numbers (ICANN) to deal with conflicts arising over domain name ownership. All registrars in the *.com*, *.net*, and *.org* domains are subject to this policy, the text of which can be accessed at ICANN's Web site at www.icann.org.

Security Considerations

It is important that bank management be alert to security considerations regarding domain name servers, which are computers that allow Internet users to locate information and resources on the Internet by domain name. These servers maintain a database of domain names and their corresponding network locations. Unauthorized changes to the server could result in misdirected Internet traffic or obstructed access to a bank's Internet site. While many banks outsource this function to third-party service providers, bank management can ensure that security features are in place and assessed periodically.

Management also can consider security in its communications with the bank's domain name registrar. For example, to prevent unauthorized changes to a bank's domain name information, management can ensure that proper controls are in place for authenticating and authorizing all requests for modifications to its registration.

For More Information

Questions and requests for additional information can be directed to Cynthia Bonnette in the FDIC Bank Technology Group at 202-736-0528 or cybonnette@fdic.gov.

Christie A. Sciacca
Director, Bank Technology Group