NATIONAL CREDIT UNION ADMINISTRATION
1775 Duke Street, Alexandria, VA 22314

DATE: December 2002 **LETTER NO.:** 02-CU-16

TO: All Federally-Insured Credit Unions

SUBJ: Protection of Credit Union Internet Addresses

ENCL: Domain Name Control Considerations

The purpose of this letter is to provide credit unions with risk management control considerations related to obtaining and maintaining an Internet address.

Internet addresses are based on registered domain names and their corresponding Internet Protocol addresses in a system coordinated by the Internet Corporation for Assigned Names and Numbers.

Many credit unions offer a website as a channel to provide services to members. However, members may not always reach the intended credit union's website, but instead reach another entity's website. Reasons vary, but include:

1. inaccurate entry of the credit union's registered domain name;

2. loss of the credit union's domain name due to untimely payment of the domain name registration renewal fee, allowing another party to obtain the domain name; and

3. redirection ("hijacking") of Internet traffic due to inadequate security practices (i.e., weak authentication procedures of the registration organization, domain name system computers using software susceptible to known vulnerabilities, etc.).

Any product or service can expose the credit union to increased risk. Risk is the potential that events, expected or unanticipated, may have an adverse effect on the credit union if not properly controlled. Risks and associated threats related to members inadvertently reaching a website other than the intended credit union's site include:

Transaction Risk – If members are lured into disclosing certain information (e.g., user identification, passwords, social security numbers, etc.), that information could be used to make fraudulent transactions or to commit identity theft.

Strategic Risk – If the credit union's Internet address is secured by a third party, the credit union's marketing investments related to website branding efforts could be negatively impacted, as could member adoption and retention rates for other Internet-based services (i.e., Internet banking, etc.) if fraud was to occur.

Compliance Risk – If members experience substantial harm due to the lack of an adequate credit union security program, the credit union may be in non-compliance with Part 748 of NCUA Rules and Regulations.

Reputation Risk – If any of the previously mentioned situations occurred, or if members were directed to a site containing offensive material, the credit union's reputation may be negatively impacted.

Credit unions with, or planning, an Internet presence are encouraged to review the enclosed guidance on risk management considerations for domain names.

Additional guidance related to information systems and technology, including Internet-based services, is available on the IS&T section of NCUA's website at http://www.ncua.gov/ref/IST/.

If you have any questions or concerns, please contact your NCUA Regional Office or State Supervisory Authority.

Sincerely,

/S/

Dennis Dollar
Chairman

Domain Name Control Considerations

When implementing an Internet presence, credit unions should establish controls to facilitate control over domain names. Credit unions should:

1. understand the Domain Name System;
2. select an appropriate domain registration organization;
3. ensure security and operational protections are in place;
4. register appropriate domain name(s);
5. become familiar with dispute resolution; and
6. file Suspicious Activity Reports when necessary.

1. Domain Name System

Each credit union's website has a unique Internet Protocol (IP) address represented by four sets of numbers separated by periods. Rather than using difficult to remember numeric addresses, a Universal Resource Locator (URL) address can be used to gain access to a website. A credit union's URL is comprised of a prefix (e.g., "www." or "http://www.") and a domain name.

Domain names incorporate credit union selected text (e.g., "abcfcu," "abcfcu-online," etc.) and a suffix called the "top-level domain" (TLD). TLDs include ".com," ".org," ".coop," ".biz," ".net," ".info," ".museum," ".aero," ".name," ".pro," ".edu," and ".gov." Other TLDs are also available, including country code (cc) TLDs (e.g., ".us," ".uk," etc.).

Domain name system (DNS) computers on the Internet maintain databases of domain names and their corresponding IP addresses. There is only one IP address associated with each domain name. This ensures "universal resolvability" - anyone, anywhere on the Internet, can use a domain name to access the intended website. For example, if the hypothetical URL www.abcfcu.org is communicated to a DNS computer, the associated IP address of 128.9.128.127 is identified as the targeted site's domain name server. This process is called "resolving the domain name."

2. Selection of Domain Name Registration Organization

The Internet Corporation for Assigned Names and Numbers (ICANN) is the non-profit coordinating body that oversees the distribution of unique IP addresses and domain

names. ICANN establishes the TLDs and accredits third parties to act as domain name "registrars." A directory of accredited registrars appears on ICANN's website at http://www.icann.org/. Accredited registrars may also offer their services through resellers.

When selecting an organization to register or maintain a domain name, credit unions should understand that registering organizations:

· establish their own pricing, which may include additional services (e.g., e-mail, website hosting, etc.);

· have websites with varying functionality and ease of use for customer self-administration of domains (e.g., changing registration information, renewing domains, etc.);

· may require responses to e-mail confirmations prior to making requested changes to registration information (e.g., website provider's IP addresses, etc.); and

· frequently offer automated services to provide notification to any party when a given domain name registration lapses. Some even offer back ordering, allowing automatic registration of a domain name the moment the current holder's registration lapses.

Credit unions can choose to register their domain name(s) themselves or contract with an outside party to perform domain name management for them. When contracting with an outside party, credit unions should remember to perform due diligence. For additional information on due diligence, please refer to NCUA Letter to Credit Unions 00-CU-11 Risk Management of Outsourced Technology Services and NCUA Letter to Credit Unions 01-CU-20 Due Diligence Over Third Party Service Providers, both available at http://www.ncua.gov/indexref.html.

To maintain control over a domain name, the credit union should consider:

· registering the domain name in the credit union's own name (versus a service provider);

· listing a credit union staff person as the administrative contact (versus a service provider contact);

· requiring credit union street and e-mail addresses (e.g., cio@abcfcu.org), versus private addresses, be listed for the administrative contact;

· remitting the payment of domain name renewal fees on time to avoid a lapse in registration which can allow a third party to purchase the domain;
· registering the domain name for more than a one year period to reduce the

· number of necessary renewals (ten years is currently the longest available registration period);
· subscribing to automatic domain name registration renewals (requires credit card information be maintained on file by the registration organization); and
· reviewing the Federal Trade Commission's consumer alert on domain name registration frauds entitled, "What's Dot and What's Not: Domain Name Registration Scams." For more information, please refer to http://www.ftc.gov/bcp/menu-internet.htm.
These steps give the credit union control to make changes (e.g., changing website hosting companies, changing registration companies, etc.), be directly responsible for domain registration renewal, reduce the likelihood of an inadvertent lapse in registration, and facilitate awareness of domain registration frauds.
3. Security & Operational Considerations
To reduce the likelihood of a hacker redirecting ("hijacking") Internet traffic to an alternate site, credit unions will want to ensure strong security practices (e.g., DNS and other software vulnerabilities monitored and addressed timely, strong authentication process for changes to domain registration information, etc.) are in place over domain name server(s). These servers are used by the registration organization, the organization hosting the credit union's website, and the hosting organization's Internet Service Provider (ISP). In some cases, the hosting organization could be the credit union's ISP, its domain name registration organization, another service provider, or possibly the credit union itself. Appropriate security measures can be determined based on completion of a comprehensive risk assessment process. For further information on risk assessment, please refer to NCUA Letter to Credit Unions 01-CU-11 Electronic Data Security Overview, available at http://www.ncua.gov/indexref.html.
Credit unions should evaluate the use of server-based digital certificates, some times called "secure server IDs." This technology offers members the means to verify that a

particular site is indeed that of the credit union. A certificate authority (CA) issues the digital certificate and acts as a trusted third party to provide this validation. It is important to understand that the Secure Sockets Layer (SSL) protocol used for securing communications across the Internet is different from the use of secure server ID. SSL does not guarantee a member is at a legitimate site, it simply means the communication with a website (whether legitimate or fraudulent) is secured to reduce the likelihood of the communication being intercepted by a third party.

Credit unions should evaluate its risk of a single point of failure regarding DNS. For example, a credit union can specify both a primary and secondary domain name server to provide authoritative DNS information. This provides a back-up server in order to avoid prolonged disruption in critical Internet services should one of the hosting organization's servers be impaired. However, some registration companies will permit additional servers to be listed, providing a theoretical increased level of continuity assurance. Please refer to the National Infrastructure Protection Center's (NIPC) December 7, 2001 Highlights Issue 11-01 for additional information on eliminating single points of failure associated with DNS. This publication is available at http://www.nipc.gov/publications/publications.htm.

Credit unions should also understand that the DNS is used for reaching e-mail addresses, as well as websites. Thus, loss of a domain name could mean a complete loss of a credit union's Internet presence – at least temporarily.

4. Register Domain Name(s)

For member convenience, a credit union will typically register a domain name that is closely associated with its marketed identity and actively communicate this to its members. In some instances, a credit union will use its trademark as its domain name. The websites of registration organizations can determine the availability of a given domain name. Many of these sites can also suggest various permutations of a domain name and identify which are currently available.

Credit unions should understand that the ".com," ".net," ".org," ".biz," and ".info" TLDs allow for unrestricted registration on a first-come, first-served basis. The ".coop" TLD is

a “sponsored” TLD with eligibility and verification requirements and is reserved for cooperative organizations.

Credit unions should also be aware that there are “pseudo” TLDs that are not endorsed by the ICANN. These may not provide universal access to a website and may require users to download special browser plug-in software to gain access to the site. Credit unions should verify which type of TLD they are purchasing and understand the functionality and dispute resolution policies surrounding them.

In some instances, another entity can obtain a domain name very similar to a credit union’s trademark or existing domain name. Examples1 include domain names with:

· similar names (e.g., abcfcu.org vs. abc-fcu.org, etc.);

· different TLDs (e.g., abcfcu.org vs. abcfcu.coop, etc.);

· “www” as part of the domain name (e.g., wwwabcfcu.org vs. abcfcu.org); and

· common misspellings of the credit union’s name (e.g., millenniumfcu.com vs. milleniumfcu.com, etc.).

The reasons for this vary, but can include:

· Legitimate use – Other parties may have appropriate business, educational or other valid reasons. One example is when the entities’ names or acronyms for the names are the same (e.g., “abc.org” might be sought by both Agricultural Benefit Credit Union and Allied Business Computer Users).2

· Profit – Individuals may register a name with the sole intent to resell the name to credit unions at exorbitant prices. “DNS parking,” “cybersquatting,” and “cyberpiracy” are terms used to describe such situations.

· Fraud – Criminals may direct unsuspecting members to a site that may appear to be the credit union’s site. However, the purpose of such sites is to obtain sensitive information such as user logon and passwords that could compromise the member’s accounts or privacy.

· Criticism – Individuals may wish to publicly communicate their dissatisfaction with a given organization.

To avoid member confusion and prevent fraud, credit unions should consider the benefits of registering multiple domain names (i.e., several TLDs, common misspellings,

etc.). Each of the registered domains can point to the same website. Credit unions should base this decision on a cost-benefit analysis.

There may be cases where the credit union determines there is a significant likelihood that members will confuse another entity's domain name with the credit union's identity or domain name. In such instances, a credit union may seek to enhance its member education efforts, consider acquiring the other domain name from its current holder, or reach some other agreement with the current domain name holder.

Credit unions should periodically identify domain names similar to the one(s) registered by the credit union that appear to be intended for fraudulent purposes. The websites of domain name registration organizations can provide assistance in this effort as they frequently offer on-line services that will show the availability of a given domain name and related permutations.

Registration information for a domain name can be determined via the "WHOIS" registry at ICANN's integrated network information center (InterNIC) website at http://www.internic.net. Performing a domain name search will reveal the URL of the registrar's own WHOIS Server. By going to the registrar's WHOIS URL and entering the domain name, one can frequently determine the registration information for the registered site.

The WHOIS registration record will disclose the name, mailing address, e-mail address, and phone number for the registrant, the administrative contact, and the technical contact. The record also lists the IP addresses for the primary and secondary hosting domain name servers, the registration date, and the registration expiration date.

Accuracy and completeness of WHOIS data can vary based on the controls of the registering organization. Additionally, due to abuses (i.e., use of data for unsolicited advertising, etc.) and privacy concerns with the WHOIS system, some registration organizations offer the use of "private" registrations. Private registrations permit a different party to be listed as the registrant, administrative contact, and technical contact. This party acts as an intermediary (or "proxy") and forwards e-mail and postal mail to the registrant according to predefined options. The proxy will disclose the

registrant's actual contact information in certain situations (i.e. to comply with legal processes, certain dispute procedures, etc.).

5. Dispute Resolution

In some cases, credit unions may decide to seek court action or administrative procedures to obtain control of a domain name.

The ".org," ".com," ".net," ".biz," ".coop," ".info," ".museum," ".name," and ".aero" TLDs follow the Uniform Dispute Resolution Policy (UDRP) established by ICANN. The policy provides for court litigation to resolve disputes. It also provides for expedited administrative procedures, via approved dispute-resolution service providers, to resolve disputes in situations where registration involves each of the following three elements:

(1) the domain name registered by the respondent is identical or confusingly similar to a trademark or service mark in which the complainant has rights;
(2) the respondent has no rights or legitimate interests with respect to the domain name; and
(3) the registered domain name is being used in bad faith.

For more information on ICANN's UDRP, as well as a list of approved dispute-resolution service providers, see http://www.icann.org/udrp/.

Although not required, having a registered trademark may be helpful in litigation or arbitration regarding domain name disputes. For more information on trademark registration, please refer to http://www.uspto.gov/, or contact legal counsel.

The Anti-Cybersquatting Consumer Protection Act, 15 U.S.C. Section 1125(d), may provide legal recourse in certain situations where the purchaser intends to profit by registering a domain name that is confusingly similar to another name.

6. Suspicious Activity Reporting

Credit unions should report suspicious activity involving domain names by completing a Suspicious Activity Report (SAR). For further information, please refer to NCUA Letter to Credit Unions 00-CU-04 Suspicious Activity Reporting, available at http://www.ncua.gov/indexref.html.