NCUA LETTER TO CREDIT UNIONS

NATIONAL CREDIT UNION ADMINISTRATION
1775 Duke Street, Alexandria, VA

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/Resources/CUs/IST/Pages/default.aspx.

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

Sincerely,

/S/

Dennis Dollar
Chairman

Enclosure