NCUA LETTER TO CREDIT UNIONS

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

DATE: October 2001 **LETTER NO.: 01-CU-12**

TO: Federally Insured Credit Unions

SUBJ: e-Commerce Insurance Considerations

Credit unions are rapidly introducing e-Commerce products and services to better meet the changing needs of their members. However, e-Commerce can significantly increase the risk exposure of those credit unions offering such services. I encourage you to evaluate your existing and optional insurance coverage to determine if your present coverage level is sufficient in light of the additional risk that may be presented by e-Commerce.

When evaluating what role insurance has in a credit union's risk strategy for e-Commerce, credit unions should understand:

- Insurance is not a substitute for strong internal controls.
- Traditional fidelity bond coverage may not protect from losses related to e-Commerce.
- Availability, cost, and covered risks of e-Commerce-specific policies vary by insurance carrier.
- Losses exceeding the insured limit could severely impact the credit union's capital position.
- Reputation risk cannot be adequately covered by insurance.

This letter addresses common questions regarding e-Commerce and insurance coverage. It is intended to highlight issues for consideration when reviewing the credit union's insurance needs relative to risks associated with e-Commerce.

How does insurance help mitigate risk?

Risk is the potential that events, expected or unanticipated, may have an adverse effect on the credit union's net worth and earnings. Uncontrolled risk-taking can prevent the credit union from reaching its objectives and can jeopardize its operations.

The key to effective risk management is an active and informed board of directors. The Board guides the credit union's strategic direction - including its risk tolerance. Insurance can assist management in its risk mitigation efforts.

What is a risk assessment?

A risk assessment is the on-going process used by management to determine the necessary activities to control risk. Appendix A of the *NCUA Rules and Regulations, Part 748, Security Program*, *Report of Crime and Catastrophic Act and Bank Secrecy Act Compliance,* outlines the following steps to assist credit unions performing risk assessments:

1) Identify internal and external threats.
2) Assess the likelihood and potential damage of the threats.
3) Assess sufficiency of policies, procedures, and other arrangements to control risk.

It is critical to perform a risk assessment prior to implementing any new product or service. A thorough risk assessment allows the credit union to develop an action plan to appropriately mitigate the risk (internal and external, controllable and uncontrollable) associated with a particular product or service. Revised or optional insurance coverage may be part of that plan.

Remember, risk exposure can change rapidly. Therefore, a risk assessment should not be a one-time event, but rather part of the credit union's on-going risk management process.

Does NCUA require insurance coverage for e-Commerce activities?

NCUA has no specified insurance requirements for e-Commerce. However, credit unions should have a risk management program in place to manage the risks inherent in their operations. Insurance can play a role in mitigating risks to an acceptable level so the strategic objectives of the credit union can be achieved.

Additionally, Part 713 of *NCUA Rules and Regulations, Fidelity Bond and Insurance Coverage for Federal Credit Unions,* requires the board of directors of each federal credit union to review its insurance coverage to ensure that it is adequate in relation to the potential risks facing the credit union. This review of insurance coverage is required at least annually. A thorough risk assessment process would assist in the determination of the adequacy of the coverage in relation to the credit union's activities – including e-Commerce.

Credit unions should reevaluate insurance needs whenever a new product, service, or vendor relationship is considered, as these may introduce new risks for which insurance coverage may need to be changed.

Does a credit union face risk if it does not have a transactional web site?

An Internet connection and e-mail alone can significantly increase the risk exposure of a credit union. These are potential avenues for virus introduction and hacking into the credit union's information systems. Having a web site simply introduces additional levels of risk that need to be addressed.

What types of risk related to e-Commerce can be insured?

The availability and extent of coverage varies by carrier. Examples of the kinds of risk for which coverage now exists in the marketplace include:

- Vandalism of credit union web sites,
- Attacks against credit union systems intended to slow or deny service,
- Loss of related income,
- Computer extortion,
- Theft of confidential information,
- Violation of privacy,
- Litigation (breach of contract),
- Destruction or manipulation of data (including a virus),
- Fraudulent electronic signatures on loan agreements,
- Fraudulent instructions via e-mail,
- Certain events impacting systems not under the credit union's control (e.g., service provider),
- Insiders who exceed system authorization, and
- Actual or threatened situations requiring the use of negotiators, public relation consultants, security consultants, programmers, substitute systems, etc.

The risks noted above are primarily addressed in optional coverage. It is important for a credit union to understand what is, and is not, covered in the policies it has in place and is considering. Exclusions in coverage may apply in a variety of circumstances.

For example, systems not under a credit union's direct operational control may not be covered by the credit union's insurance protection. As discussed in *NCUA Letter to Credit Unions 00-CU-11, Risk Management of Outsourced Technology Services*, credit unions should consider contractual provisions regarding insurance coverage to be maintained by the service provider.

What type of policy covers the risk associated with e-Commerce?

The risk associated with e-Commerce is wide-ranging and can be covered in various places within an insurance carrier's product offerings such as the fidelity bond, electronic computer crime coverage, and other optional coverage. Each type of coverage should

be reviewed closely to determine if it is adequate in relation to the credit union's risk exposure.

- Fidelity bond coverage principally serves to cover the direct loss due to a physical crime such as theft of certain defined property (e.g., negotiable items) stolen by a first party (e.g., employee from an employer).

- Electronic computer crime coverage serves to fill some of the gaps in fidelity bond coverage. It typically covers the direct loss due to an electronic computer crime resulting in the loss of defined property (e.g., negotiable items). Moreover, it can cover the risk of viruses and the manipulation or destruction of data and programs.

- Other optional coverage serves to fill some of the gaps in the fidelity and electronic computer crime coverage. These may cover indirect losses (e.g., business interruption/resumption and extortion) and expand defined property to include confidential member and credit union data. Some may cover additional related liabilities or expenses, even in relation to external service providers or litigation.

Coverage varies among insurance carriers, and carriers often bundle their insurance offerings in different packages with unique marketing names. The coverage afforded by these policies may change in the future based on the insurance industry's perceived risk and claims experience.

Why are strong internal controls related to e-Commerce needed if insurance coverage is in place to reduce risk?

Insurance alone is not enough. Strong internal controls are necessary for many reasons, including:

- Insurance carriers may require a reasonable level of controls be in place in order to obtain coverage.
- Insurance coverage will not cover losses over a predetermined dollar limit.
- A credit union may not be covered for certain losses.
    - e-Commerce related policies are evolving and coverage for certain risks may be available only under separate optional policies, which the credit union may or may not have purchased.
    - Existing coverage can change. For example, all carriers may not cover losses related to viruses in the future.
- Future insurance cost to the credit union may increase based on claim experience.
- Reputation of a credit union cannot be adequately protected via insurance. It takes time to build trust, but it can be lost relatively quickly.

- *Part 748 of NCUA Rules and Regulations* requires a security program (including a system of internal controls) to protect member data.

Credit unions are encouraged to evaluate their current insurance coverage with regards to e-Commerce activities. When properly used in its role to supplement an effective system of internal controls, insurance can be a key component of the credit union's risk mitigation strategy. In this manner, insurance can help protect credit unions and their members, while facilitating the long-term success of e-Commerce for the credit union industry.

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

Sincerely,

/s/

Dennis Dollar
Chairman