NCUA LETTER TO CREDIT UNIONS

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

DATE: October 2000 **LETTER NO.: 00-CU-07**

TO: Federally Insured Credit Unions

SUBJ: NCUA's Information Systems & Technology Examination Program

ENCL:
(1) Appendix
(2) e-Commerce Questionnaire (EC1)
(3) e-Commerce Review Program Form (EC2)
(4) Electronic Data Processing Review Form (EDPR)

NCUA has developed and implemented Phase I of its Information Systems & Technology Examination Program (ISTEP). Phase I of the program focuses on electronic financial services and more specifically, e-Commerce services (see the Appendix for definitions). If your credit union offers e-Commerce services to its membership, federal or state examiners may use the ISTEP during the examination of your credit union. The ISTEP tools provided to examiners include the following:

- e-Commerce I (EC1): High level e-Commerce questionnaire for reviewing e-Commerce services and activities.
- e-Commerce II (EC2): Detailed questionnaire for reviewing e-Commerce services and activities.
- EDP Review (EDPR): Electronic Data Processing review program for reviewing a credit union's overall information and technology systems.

Examiners will use EC1 if your credit union provides e-Commerce services. Examiners may also use EC2 to address areas not sufficiently covered by EC1 or in those instances where your operating environment and services provided suggest a more in-depth review is advisable. Examiners may also elect to use the EDPR to conduct a general review of your electronic data processing systems.

For your information, I have enclosed with this Letter copies of the two e-Commerce questionnaires and EDPR program. Since technology changes at a rapid pace, NCUA expects to update the program as needed to keep pace with those changes. The most

recent version of the program will be continuously available for download from our website (www.ncua.gov).

In the near future and ongoing, NCUA will issue Letters to Credit Unions, guidance papers, and articles specifically addressing information systems and technology issues. These documents will also be available for download from our website.

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

Sincerely,

_____/s/_____
Norman E. D'Amours
Chairman
National Credit Union Administration Board

Enclosures

Appendix

For the purposes of this Letter, the following definitions apply:

- Electronic Financial Services (EFS): EFS includes those services that a credit union provides via electronic means including, but not limited to, the following:
  - Electronic Commerce Systems:
    - Website Systems (World Wide Web or Internet/Browser Based)
    - Home Banking/PC Based
    - Audio Response/Phone Based
    - Wireless
    - Kiosk
  - Electronic Payment Systems:
    - ACH Transactions
    - Stored Value Cards
    - Electronic Money
    - Electronic Wallets
  - ATM Systems
- e-Commerce Services: e-Commerce includes those services that a credit union provides, and a member accesses, via electronic means including, but not limited to, the following:
  - Internet/World Wide Web Services
  - Wireless Services
  - Home Banking (direct dial in) Services
  - Online Bill Paying Services
  - Account Transaction Processing Services:
    - Account Inquiry
    - Check Requests
    - Loan Applications
    - Bill Payment
    - Funds Transfers
    - 3rd Party Transfers
    - On-Line Wire Transfers
    - Automated Clearing House (ACH) Originations

Credit Union:
Charter #:

E-Commerce Questionnaire (EC-1)

Sec. #	Que. #	Sub-Que. #	Question	Y/N/ NA/ NR	Comments
1	**General**				
1	1	0	Does the credit union engage in E-Commerce activities with its members via the Internet, world-wide web, home banking, etc.		
1	2	0	Are E-Commerce products and services considered to be critical to the credit union's goals and strategies?		
1	3	0	Have adequate policies and procedures been developed for the credit union's E-Commerce activities?		
1	4	0	Does the credit union have an E-Commerce organization chart or listing of key E-Commerce staff?		
1	5	0	Has management established an E-Commerce oversight committee comprised of representatives from applicable departments such as Marketing, Compliance, Operations, Information Systems and Security?		
1	6	0	Does the credit union Board of Directors receive reports on E-Commerce activities on a regular basis?		
1	7	0	Does the credit union have an a) informational, b) interactive or c) transactional website?		
1	8	0	Is the website hosted by a) the credit union, b) vendor or c) third party?		
1	9	0	Is the website content developed and maintained by the credit union?		
1	10	0	Does the credit union offer the following services electronically:		
1	10	1	Member Application		
1	10	2	Share Account Application		
1	10	3	Share account transfers		
1	10	4	Loan Applications		
1	10	5	Loan payments		
1	10	6	Bill payment		
1	10	7	Account Balance Inquiry		
1	10	8	View Account History		
1	10	9	Download Account History		
1	10	10	Share Draft Orders		
1	10	11	Merchandise Purchase		
1	10	12	Electronic Cash		
1	10	13	Wire Transfers		
1	10	14	Other (describe)		
2	**Risk Assessment**				
2	1	0	Are there policies, procedures and practices in place for performing risk assessments to identify internal and external threats and vulnerabilities associated with E-Commerce?		
2	2	0	Do these policies and procedures address Operational/Transactional, Security, Reputation and Compliance Risks?		
2	3	0	Has a risk assessment been performed for the credit union's E-Commerce activities?		
2	4	0	Does management actively reevaluate risks associated with technological and operational changes in E-Commerce?		
2	5	0	Has management considered and is it continually monitoring the risks associated with outsourcing relationships?		
3	**Compliance and Legal**				
3	1	0	Is legal counsel consulted for significant matters such as E-Commerce contracts, partnerships and affiliations?		
3	2	0	Are changes to applicable laws and regulations actively monitored and are policies and procedures updated accordingly?		
3	3	0	Have appropriate procedures been put in place to ensure that E-Commerce transactions are legally binding (e.g., verifiably performed by the appropriate party) and cannot be repudiated?		
3	4	0	Has management determined whether E-Commerce activities are included in its bond coverage and, if so, has management determined if the coverage is sufficient?		
3	5	0	Does management review the credit union's bond coverage annually to ensure that it is adequate in relation to the potential risk?		
3	6	0	Has management considered the legal ramifications associated with providing E-Commerce services to multi-state and multinational members?		
4	**Audit and Consulting Services**				

Credit Union:
Charter #:

E-Commerce Questionnaire (EC-1)

Sec. #	Que. #	Sub-Que. #	Question	Y/N/NA/NR	Comments
4	1	0	Are E-Commerce activities subject to periodic internal (internal audit) and/or external (SAS 70 or financial statement) audits and quality reviews?		
4	2	0	Has management prioritized the issues disclosed in the most recent audit or quality review?		
4	3	0	Has management corrected, or is in the process of correcting, these issues?		
4	4	0	Has management performed and documented an assessment to determine if Attack and Penetration Testing should be used as a means of identifying, isolating and confirming possible flaws in network and security architecture?		
4	5	0	If the assessment warrants penetration testing, has management performed, contracted or planned to contract for these services?		
4	6	0	If a penetration test has been performed, has management addressed, or is in the process of addressing, identified vulnerabilities?		
5	**Vendor Management**				
5	1	0	Has management assessed long-term strategic and short-term tactical plans for current and future E-Commerce outsourcing activities?		
5	2	0	Does management actively monitor whether critical, outsourced service providers continually meet the credit union's E-Commerce needs (i.e. hardware, software, network services)?		
6	**Member Service and Support**				
6	1	0	Does management have a process in place to adequately track and resolve member support issues (e.g., member technical support, incident reports, and FAQ's)?		
6	2	0	Has management established and tailored member service level goals based on their business needs and unique field of membership expectations?		
7	**Personnel**				
7	1	0	Is the credit union adequately staffed and trained with respect to its E-Commerce strategy?		
7	2	0	Does an adequate segregation of duties exist between conflicting E-Commerce related responsibilities?		
7	3	0	Does the credit union have a process in place to handle the addition, modification or deletion of employee's access due to status changes, i.e. terminations, transfers, promotions?		
7	4	0	Has credit union management implemented practices to address the recruitment and retention of E-Commerce technical staff?		
8	**System Architecture and Controls**				
8	1	0	Are adequate network, system and application diagrams (i.e. topologies) maintained?		
8	2	0	Is an adequate inventory of E-Commerce hardware and software maintained?		
9	**Security Controls**				
9	1	0	Does the credit union have an adequate security program in place (i.e., documented policies and procedures) which covers protecting critical data and facilities?		
9	2	0	Does management monitor credit union staff activity to ensure compliance with established security policies and procedures?		
9	3	0	Have safeguards been implemented to mitigate the risk of confidential member and servicing information being disclosed to or modified by unauthorized users?		
9	4	0	Have authentication techniques/controls been put in place to block unwanted communications into and out of the credit union network (i.e., Firewall)?		
9	5	0	Have member session controls been put in place to ensure that access is only granted to the appropriate users?		
9	6	0	Have controls been put in place that automatically log-off a session (member or other users) as a result of inactivity?		
9	7	0	Has management classified data based upon its sensitivity, perceived value and the impact to management in the event of its loss?		
9	8	0	Have the various types of data communicated on the credit union's network been categorized according to its sensitivity?		
9	9	0	Has the credit union implemented adequate security policies and procedures according to the sensitivity and importance of data?		
9	10	0	Is a criteria in place which determines the level of encryption that shall be used for the varying degrees of sensitive information?		

Credit Union:
Charter #:

E-Commerce Questionnaire (EC-1)

Sec. #	Que. #	Sub-Que. #	Question	Y/N/ NA/ NR	Comments
9	11	0	Is an appropriate level of encryption being utilized to protect sensitive data (data residing on the webserver or transmitted during a session)?		
9	12	0	Are effective and thoroughly tested security tools used to monitor internal and external threats?		
9	13	0	Does the credit union ensure that virus identification and protection software is implemented, monitored and updated when required?		
9	14	0	Does the credit union have an intrusion detection system?		
9	15	0	If yes, is it a real-time intrusion detection system?		
9	16	0	Does the credit union respond to potential intrusions in a timely manner?		
10	**Business Continuity**				
10	1	0	Has disaster recovery relating to E-Commerce been incorporated into the credit union's overall business continuity plan?		
10	2	0	Does the credit union review its plan, at least annually, based on changes in technology, its infrastructure or E-Commerce activities?		
10	3	0	Is the plan tested on a regular basis and are the test results analyzed to identify necessary changes?		
10	4	0	Has the credit union developed incident response and escalation procedures for technical, security or member concerns?		
11	**Performance Monitoring**				
11	1	0	Has the credit union established and implemented adequate performance monitoring procedures for E-Commerce activities?		
11	2	0	Is the performance of E-Commerce activities monitored by management against long-term and short-term plans, or member demands?		