SAMPLE CREDIT UNION INFORMATION SECURITY
DUE DILIGENCE QUESTIONNAIRE FOR POTENTIAL VENDORS

Section 1
CREDIT UNION Member Information Security Due Diligence Questionnaire

1. Physical security
- Where is (are) your data center(s) located?
- Describe the physical security, disaster recovery, backup/redundancy, and prevention features of your data center.
- Who (including data center staff, other employees and vendors) has physical access to the host servers?

2. Network security
- Are industry-standard firewalls deployed? Where are they deployed? How does your company keep the software for the firewalls current? Is administrative access to firewalls and other perimeter devices allowed only through secure methods or direct serial port access?
- What protocols and ports are allowed to traverse the network and firewall?
- Are public facing servers contained in a DMZ?
- Is the internal network separated into different security VLANs?
- Does your company use intrusion detection systems (IDSs)? How long are IDS logs kept?
- Does your company use an intrusion prevention system (IPS)?
- Does your company deploy host based intrusion prevention systems (HIPS)?
- Does your company actively review logs or have a system that can correlate all logs from systems and provide accurate event alerting?
- Are formal incident-response procedures in place? Are they tested regularly?
- Does your company engage third-party security service providers to perform ongoing vulnerability assessments?
- Does your company have a workflow diagram of the process for CU system failure? If so, please provide.

3. Systems security
- Are ongoing vulnerability assessments performed against the systems? If so, please provide your last assessment results and/or executive overview for review once we are on-site. If you do not agree to share the results of this report please explain the reasons why.
- How are operating systems kept up to date? How does your company keep abreast of software vulnerabilities? What is the procedure for

installing software updates?
- Are audit logs implemented on all systems that store or process critical information? How often are these logs reviewed?
- What change management procedures are in place?
- Does your company engage third-party security service providers to perform ongoing penetration tests? What was the scope of the test (i.e. internal, external, social engineering, blackbox)? Can you provide your last penetration test results and/or executive overview once we are on site? If you do not agree to share the results of this report, please explain why.
- Does your company have adequate data base security and/or encryption on sensitive information?

4. **Staff security**
- What are the credentials of the systems administration staff?
- Has the systems administration staff undergone complete background and criminal checks?
- Are hosting staff onsite or on-call 24/7?

5. **Security policy**
- Describe the user account and password policy. How many characters must a password have? Are alphanumeric passwords required? How frequently must it be changed?
- Are screen-blanking mechanisms deployed on all employee workstations? Do sessions automatically time out after an idle period?
- Are user accounts for contract personnel created with expiration dates? How are user accounts closed after termination?
- How long are the access logs retained for? Who reviews the logs?

6. **Software overview** (if possible, please send a copy of the software or provide access to a version for evaluation)
- Please provide a description of any software that is required for credit unions to use in order to support your products/services.
- Does the software require an interface with our core processing system?
- Does the software allow your company access to any credit union data via download and/or direct interface?
- Does your company conduct code reviews?
- Are your developers trained in secure coding? Please explain.
- Are all development software licenses current? Please provide a list of your development software licenses. Does your company utilize any third-party software development companies? If so, please explain.
- When was the software first released? When was the software last updated? How often are software updates/upgrades planned? Does the credit union pay for updates/upgrades?

7. **Privacy/confidentiality of data**
- How does your company protect the privacy of any member and/or

account information that may be collected through this service?
- Is your company SAS 70 certified?
- Is your company ISO 27001 or 27002 (previously 17799) compliant?
- How is data integrity ensured? What checks are carried out on people who might have access to the data?
- Discuss all security features built into the software.
- Please describe the levels of support (i.e., technical, customer, etc.) your company provides to participating credit unions. What methods would a credit union use to contact your company for support? How many staff positions are available to assist credit unions with support issues?
- What happens to CREDIT UNION data if we terminate the service with your company?
- Will any CREDIT UNION data or systems be subcontracted to or handled by another vendor or service provider? If so, please provide details of this arrangement regarding which parts of the system will be subcontracted, what data will be shared, how the data will be shared, and any supporting service level agreements with your subcontractor(s).

Section 2
Website and/or Application Service Provider Member Information Security Due Diligence

CREDIT UNION Application Service Provider Policy and Security Standards For Third Party Applications

1.0 Overview

This portion of the questionnaire collects security criteria that an Application Service Provider (ASP) must provide in order to be considered for use by the Credit Union. As part of the ASP selection process, the Vendor must respond in writing to EVERY statement and question in section *4.0 Standards*. CREDIT UNION's Information Security Group will closely review the vendor responses, and may suggest remediation measures in any areas that fall short of the minimum-security criteria. Approval of any given ASP resides largely on the vendor's response to this document.

2.0 Scope

This document can be provided to ASPs that are either being considered for use by Credit union, or have already been selected for use.

3.0 Responding to These Standards

Credit union's Information Security Group is looking for explicitly detailed, technical responses to the following statements and questions. ASPs should format their responses directly beneath the Standards (both questions and requirements) listed below. In addition, please include any security whitepapers, technical documents, or policies that you may have.

Answers to each of the questions in the following section should be specific and avoid generalities.

4.0 Standards

4.1 General Security

1. Credit union reserves the right to periodically audit your application infrastructure to ensure compliance with the ASP Policy and these Standards. Nonintrusive network audits (basic portscans, and basic Web Application Inspection etc.) may be done randomly, without prior notice. More intrusive network and physical audits may be conducted on site with 72 hours notice. Will this be acceptable to your company?
2. The ASP must provide a proposed architecture document that includes a full network diagram of your Application Environment, illustrating the relationship between the Environment and any other relevant networks, with a full data flowchart that details where Credit union data resides, the applications that manipulate it, the security thereof, and network security including any devices using Access Controls.
3. Does access to any Credit union system or data utilize the *"principle of least privilege"*? The principal of least privilege states the following: both the application and users operate under the minimum amount of access rights needed to produce the task.
4. Can your company immediately disable all or part of the functionality of the application should a security issue be identified?

4.2 Physical Security

1. Describe the physical security protecting the equipment hosting the application for Credit union.
2. Please list all parties (by position or by association with your company) that will have access to the environment hosting the application for Credit union.
3. Provide a description of your employee and contractor background check procedures and approvals.

4.3 Network Security

1. Is the network hosting the application air-gapped from any other networks or customers that the ASP may have? If not, please indicate what infrastructure will be shared with other ASP customers.
2. What data will be transmitted between Credit union and the ASP?
3. How will data be transmitted between Credit union and the ASP?

4.4 Host Security

1. The ASP must disclose how and to what extent the hosts (Windows, Unix, Linux, etc.) comprising the ASP application infrastructure have been hardened against attack. If the ASP has hardening documentation for this procedure, provide that as well.
2. The ASP must provide a listing of current patches on hosts, including host OS patches, web servers, databases, and any other material application.
3. Provide processes and policies describing how and when security patches are evaluated and applied.
4. Provide a document outlining a Service Level Agreement (SLA) in place that will

specify a time frame in which we can expect vulnerabilities to be fixed, or patches to be applied? This SLA will be need separate CREDIT UNION approval specifically from the Information Security Group.
5. Describe the processes used for monitoring the integrity and availability of those hosts.
6. Provide the password policy information for the Credit union application infrastructure, including minimum password length, password generation guidelines, and how often passwords are changed.
7. Describe the account generation, maintenance and termination process, for both maintenance as well as user accounts. Include information as to how an account is created, how account information is transmitted back to the user, and how accounts are terminated when no longer needed.

4.5 Web Security

1. Will the ASP disclose the specific configuration files for any web servers and associated support functions (such as search engines or databases)?
2. Please disclose whether, and where, the application uses Java, Javascript, ActiveX, PHP or ASP (active server page) technology.
3. What language is the application back-end written in, (C, Perl, Python, VBScript, etc.) and what Data Base is being utilized.
4. Please describe the ASP process for doing security Quality Assurance testing for the application. For example, testing of authentication, authorization, and accounting functions, as well as any other activity designed to validate the security architecture.
5. Has the ASP done web code review, including CGI, Java, etc, for the explicit purposes of finding and remediating security vulnerabilities? If so, who did the review, what were the results, and what remediation activity has taken place? If not, when is such an activity planned?

4.6 Cryptography

1. The Credit union application infrastructure cannot utilize any "homegrown" cryptography. Any symmetric, asymmetric or hashing algorithm utilized by the Credit union application infrastructure must utilize algorithms that have been published and evaluated by the general cryptographic communities.
2. Encryption algorithms must be of sufficient strength to equate to 256-bit AES.
3. Are hashing functions employed? Which algorithms are used (i.e. SHA-2 or MD5)?
4. Will Credit union systems connect to the ASP through the Internet? If so, please describe. What encryption methods will be used?
5. Will the ASP application infrastructure require PKI?