NCUA LETTER TO CREDIT UNIONS

NATIONAL CREDIT UNION ADMINISTRATION
1775 Duke Street, Alexandria, VA

DATE: **July 2002** **LETTER NO.: 02-CU-13**

TO: **Federally Insured Credit Unions**

SUBJ: **Vendor Information Systems & Technology Reviews – Summary Results**

ENCL:
(1) Appendix A: Summary of Vendor Information Systems & Technology Reviews
(2) Appendix B: Vendor Report, Frequently Asked Questions (FAQ's)
(3) Appendix C: Rating Definitions

As part of NCUA's Credit Union Vendor Review Program during 2001, the agency conducted ten credit union vendor information systems and technology (IS&T) reviews. Nine of these reviews were conducted under the authority provided by the Examination Parity and Year 2000 Readiness for Financial Institutions Act (Exam Parity Act)[1]. The purpose of this letter is to provide you with a high-level summary of the issues, concerns, and trends evidenced from those reviews. The vendors reviewed were:

Vendor	Location	Review Date
Apex Data Systems, Inc.	Indianapolis, IN	12/17/2001
Computer Marketing Corp.	Salt Lake City, UT	12/31/2001
Computer Consultants Corp.	Salt Lake City, UT	01/14/2002
CU Solutions, Inc.	Fort Mill, SC	12/13/2001
EPL, Inc.	Birmingham, AL	09/24/2001
FedComp, Inc.	Fairfax, VA	07/20/2001
Liberty Enterprises, Inc.	Roseville, MN	12/08/2000
Share One, Inc.	Memphis, TN	11/05/2001
SOSystems, Inc.	Orem, UT	11/29/2001
Western New York Computing Systems, Inc.	Penfield, NY	12/19/2001

[1] NCUA's authority under the Exam Parity Act expired December 31, 2001. Any review conducted after that date was voluntary on the part of the vendor.

The vendor IS&T reviews focused primarily on e-Commerce applications and initiatives provided and/or supported by the vendor. The IS&T scope also included a review of the vendor's overall operations (management and technical), a high-level analysis of its current financial condition, the adequacy of its capital, and the ability of the enterprise to continue as an ongoing concern.

NCUA's objectives for the on-site reviews were to:

- perform a high-level review of the vendor's infrastructure;
- identify and assess the vendor's information systems and technology risks, with specific emphasis on its network services, web-hosting, and Internet account services;
- gain insights on current issues that vendors and the credit union industry are facing regarding emerging technologies; and
- provide recommendations for areas of improvement.

During the on-site visit, we performed the following steps:

- conducted an introductory meeting to apprise management of the review objectives and process;
- interviewed key staff to identify and evaluate information systems risks, issues, and concerns;
- reviewed documentation regarding strategic information technology (IT) efforts;
- analyzed findings and developed the review report; and
- conducted an exit meeting with management to discuss observations and recommendations.

At the conclusion of the review process, NCUA issued a draft report to the vendor, provided the vendor the opportunity to comment on the observations noted in the report, and issued a final report to the vendor, its credit union customers of record, NCUA staff, and applicable State Supervisory Authorities (see Appendix B for a discussion on report distribution and other frequently asked questions). As part of NCUA's risk-focused examination program, examiners may use the vendor reports to help them assess the technology and other related risks associated with outsourcing arrangements.

Overall, the vendors reviewed were committed to the goal of providing quality services and products to their customers. The vendors were also receptive to recommendations and suggestions and, when practical, implemented recommended changes prior to completion of the review.

Many vendors shared some similar common underlying weaknesses. It is noteworthy that the impact and associated risks of those weaknesses tended to vary from vendor to vendor due to each vendor's unique operational environment (technical, managerial, financial, etc.). The key common weaknesses identified were:

- ***Risk Assessment*** – Eight vendors either lacked an enterprise-wide risk assessment process or the existing process did not encompass all operational areas.
- ***Information Security Policies & Procedures*** – Eight vendors needed to develop or improve their policies and/or procedures regarding the protection of information stored on, or transmitted through, their systems.
- ***Operating Policies & Procedure***s – All vendors needed to develop or update existing policies to reflect current operations.
- ***Disaster Recovery Plan Testing*** – All vendors needed to enhance their disaster recovery plan testing procedures and controls.
- ***Incident Response*** – Six vendors lacked a formal and detailed incident response plan and/or incident response procedures needed to be improved. In addition, eight vendors needed to improve their ability to detect an intrusion or other incident.
- ***Internet Commerce Application*** – Six vendors needed to revise their service level contracts with their credit union customers to include and/or cover rights and responsibilities for the Internet commerce product. Six vendors needed to improve session management controls to enhance security and privacy. Five vendors needed to improve the application's member privacy controls.
- ***Financial Audit*** – Seven vendors did not have audited financial statements.

A further discussion on the preceding issues, as well as a list of additional common issues, may be found in Appendix A.

Each vendor received an overall rating (see Appendix C for the overall rating definitions) which we disclosed in the report. No vendors received an *Unsatisfactory* rating.

NCUA's vendor report represents a high-level review as of the dates of the on-site contact at the vendor and should not be construed as an audit. Technology issues, concerns, threats, and vulnerabilities may change on a daily basis. The vendor report is another tool to assist you in managing your vendor relationships. ***NCUA's vendor report does not alleviate your responsibility to oversee and manage your vendor outsourcing arrangements.*** Please review NCUA Letter to Credit Unions 00-CU-11, Risk Management of Outsourced Technology Services, for guidance on managing relationships with technology vendors. NCUA also encourages you to frequently visit its Information Systems & Technology web page (www.ncua.gov/ref/IST/) for additional IS&T related information, news, and guidance.

For 2002, NCUA is scheduling reviews for an additional ten vendors. Since NCUA's authority under the Exam Parity Act has expired, we will conduct these reviews on a voluntary basis. For those vendors which elect not to participate, NCUA will provide notice that the vendor elected not to participate in NCUA's Vendor Review Program.

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

Sincerely,

/S/

Dennis Dollar
Chairman

Enclosures

Appendix A: Summary of Vendor Information Systems & Technology Reviews

Key Areas Reviewed

NCUA grouped results of our review procedures into the following 12 general categories and assigned a risk level (L-Low, M-Medium, H-High) for each concern listed in the report:

1. Risk Assessment
2. Information Security
3. Operating Policies & Procedures
4. Business Continuity & Disaster Recovery
5. System Development Life Cycle and Change Management
6. Personnel
7. Incident Response Capabilities
8. Technology Management
9. Strategic Direction
10. Customer Service & Support
11. Internet Application
12. General Enhancements

In some cases, a particular concern could relate to more than one category. In those situations, we cited the concern in the most relevant category, provided its impact on all the affected categories were similar. For those instances where a particular concern affected multiple categories in a different manner, we listed and discussed that concern in each of the appropriate categories.

Vendor Considerations

Though the same concern may exist for two vendors, we may have rated its impact on each vendor differently based upon their operational environment, information systems environment, application design and function, and management oversight. For example, the Summary Results Table (in the following section) cites a concern in the area of database encryption in 60% of the vendors reviewed. This citation does not mean that 40% of the vendors use database encryption; rather, it means 60% of the vendors:

- do not use database encryption and should (due to how the system operates, the type of data involved, and/or where the data resides on the system(s)); or
- use database encryption but not at a level commensurate with the level of data sensitivity and/or exposure.

Summary of Results

The table below lists the most frequent areas of concern (those areas in which 50% or more of the vendors demonstrated a weakness). The descriptions for the column headings are:

- Area of Concern – The area in which the vendor demonstrated a need for improvement.

- Vendors – The percentage of vendors that exhibited the area of concern.
- Risk Rating – The number of vendors that fell into each risk category (low, medium, or high).
- Aver. Score – The numerical average risk rating score (1-Low, 2-Medium, 3-High) for the vendors that exhibited the area of concern.

		Risk Rating			
Area of Concern	**Vendors**	**Low**	**Med.**	**High**	**Aver. Score**
Risk Assessment					
Enterprise Wide	80%		7	1	2.13
Information Security					
Comprehensive Policies & Procedures	80%	1	7		1.88
Database Encryption	60%		4	2	2.33
Virus Protection (Remote Users)	50%		4	1	2.20
Physical Security Controls	50%	1	3	1	2.00
Operating Polices & Procedures					
Formal Documentation	100%	8	2		1.20
Business Continuity & Disaster Recovery					
Disaster Recovery Testing	100%	4	6		1.60
Software Escrow	50%		5		2.00
Personnel					
Formal Training Plans	60%	5	1		1.17
Hiring Controls	50%	2	3		1.60
Incident Response					
Proactive/Detective Controls	80%		1	7	2.88
Incident Response Plan	60%		5	1	2.17
Customer Service & Support					
Customer Awareness Education	50%	4	1		1.20
Internet Commerce Application					
Service Level Contracts	60%	3	3		1.50
Session Management Controls	60%		3	3	2.50
Member Privacy Controls	50%	1	3	1	2.00

Appendix B – Vendor Report
Frequently Asked Questions (FAQs)

1. **When will I receive a copy of the vendor report?**
   The final report is generally completed 6 weeks after the onsite contact is completed. During this period, NCUA issues a draft report and provides the vendor approximately 30 days to provide comments. After receiving the vendor's comments, NCUA issues the final report to the vendor and its customer credit unions of record as of the time the on-site review was conducted.

2. **What do I do if I haven't received a copy of my vendor's report?**
   If you are a customer of the vendor, contact your NCUA Regional Office to request a copy. The Regional Office will verify with the vendor that your credit union is a customer and forward a copy of the vendor report to your credit union's address on file with NCUA.

3. **I am not a customer of the vendor but our credit union is considering converting to their product. How do I get a copy of the vendor's report?**
   Only customers of the vendor may receive a copy of the report. Prospective customers are not entitled to receive a copy. Once a prospective credit union customer signs a binding contract to convert to a vendor's system, NCUA considers the credit union a customer of that vendor and may request a copy of the report as outlined in #2 above.

   Note: For guidance on selecting vendors and managing vendor relationships, please see NCUA Letters to Credit Unions #01-CU-20, Due Diligence Over Third Party Service Providers, and #00-CU-11, Risk Management of Outsourced Technology Services.

4. **May I obtain a copy of the report directly from the vendor?**
   No. The vendor is not authorized to release the report or any portion thereof. Only NCUA's offices may distribute and/or provide a copy of the report.

5. **May I obtain a copy of the report from my examiner?**
   No. Examiners are not authorized to release vendor reports. To obtain a copy, contact your NCUA Regional Office.

6. **May I share the report and/or its contents with others?**
   The report copy is the property of the National Credit Union Administration and is furnished for the confidential use of the reviewed organization and its contracted customers. You may share the report and/or its contents with your credit union management and staff as deemed necessary. Under no circumstances shall any recipient of the report make public the report or any portion thereof. The law

provides penalties for unauthorized disclosure of any of the contents of the report. If a subpoena or other legal process is received calling for the production of the report, NCUA must be notified immediately.

7. **May I discuss the contents of the report with my examiner?**
   Yes. Should you have questions concerning the report, your examiner may be able to help you understand the issues discussed in the report. However, your examiner most likely did not participate on the vendor review contact and probably has no additional information other than that provided in the report.

8. **May I discuss the contents of the report with my vendor?**
   Yes. If you have questions concerning the status of the contents of the report, you should communicate them to your vendor.

Appendix C – Rating Definitions

SATISFACTORY
Performance is *Satisfactory* when weakness(es) is minor in nature and management demonstrates the ability to adequately correct the weakness(es) within a reasonable timeframe. Management demonstrates sufficient control over all facets of key operational areas such as: risk assessment, policies and procedures, product development and delivery, customer support, information technology security, financial stability, and business continuity and disaster recovery.
NEEDS IMPROVEMENT
Performance is *Needs Improvement* when weakness(es) is moderate in nature and the vendor demonstrates less than satisfactory, but not unsatisfactory, performance. Weakness(es) may exist that causes management to fail in meeting established goals and timeframes. Weakness(es), or the combination of weaknesses, does not threaten long-term operational or financial stability. Management demonstrates the ability to comprehend and address the weakness(es), commits to an adequate course of action, and commits to, or procures, sufficient resources to effectively deal with the weaknesses.
UNSATISFACTORY
Performance is *Unsatisfactory* when weakness(es) is significant in nature and management has not demonstrated the ability to adequately correct the weakness(es) within a reasonable timeframe. Management is not responsive, lacks commitment, or fails to comprehend the significance of the weakness(es). One or more weaknesses may have a significant or material negative impact on one or more key operational areas. The short- or long-term operational or financial stability of the vendor may be in jeopardy.