ALM | CREDIT UNION TIMES

Protecting Your CU in Core Processing & Outsourced Technology Contracts

By Charles J. Nerko

One of the biggest risks credit unions face comes from the vendors they trust to help with their day-to-day operations. Core processors and other third-party vendors are often perceived as experts by the credit unions that hire them, but that perception can breed unwarranted complacency. Outsourced technology providers have been known to expose credit unions to substantial security risks. And even the largest core processors have been known to make computational errors that result in inaccurate records.

To protect themselves and their members, credit unions need to negotiate comprehensive vendor contracts that clearly outline the vendor's responsibilities and place liability on the vendor for any problems that surface. Without a solid contract, credit unions could face immense legal liability for problems caused by their vendors.

For example, if a vendor's code infringes on a patent, the credit union may end up facing an expensive intellectual-property infringement lawsuit because the credit union uses the infringing code. And if a vendor causes a data breach or miscomputes account records, the credit union could be on the hook for expensive consumer class action lawsuits.

Charles J. Nerko

It's crucial for credit unions to make sure their core processing contracts and other outsourced technology agreements shift liability to the culpable vendor and protect the credit union from these types of liabilities. The following three best practices can help a credit union avoid costly lawsuits and protect its members:

1. Specify clear performance standards. Contracts should thoroughly lay out the vendor's responsibilities and the credit union's rights to audit the vendor. The contract should set detailed

expectations with measurable performance benchmarks while allowing enough flexibility to adapt to emerging cybersecurity risks and changes in law.

Credit unions should use information uncovered in the due diligence process to shape the performance standards set forth in the contract. Take a look at the vendor's litigation history to see if they've caused problems for other credit unions or banks in the past. This information can help credit unions avoid dealing with troublesome vendors or craft performance standards that avoid similar issues. Many of the most revealing details from past litigation are not available through web searches, so credit unions should turn to an attorney capable of performing a nationwide court docket search to analyze this data.

2. Set remedies that incentivize the right behavior. The contract should include reporting processes, escalation procedures and remedies for nonperformance that motivate the right behavior. The vendor should be held accountable for their service offerings and compensate the credit union appropriately when the vendor falls short.

3. Secure a meaningful indemnity. An indemnity means that the vendor should be responsible for legal claims that arise due to their technology. Without a properly crafted indemnity, the credit union could end up assuming liability for issues that should have been the vendor's responsibility.

Make sure the indemnity can be deployed in actual practice. Some core processors will provide an indemnity if they generate inaccurate records, yet, far down in an unrelated section of the

Source: Shutterstock

contract, hide a requirement for the credit union to review all its records and report discrepancies by the next business day. This onerous requirement renders the indemnity meaningless. Further, credit unions should review the vendor's insurance policies to ensure the indemnity has appropriate financial backing.

In summary, technology contracts are critical risk management tools for credit unions. It's important to have an experienced technology attorney craft and review these agreements to make sure they are appropriately detailed and protective. And when problems arise, experienced technology litigators can help credit unions secure financial recoveries from their vendors.

Charles J. Nerko *is leader of the data security litigation team and a partner in the commercial litigation and financial institutions and lending practice areas at the law firm of Barclay Damon LLP. Charles is resident in the firm's New York City office.*

BARCLAY DAMON LLP

cnerko@barclaydamon.com, 212.784.5807