Featured Professionals

Nadja Baer

Caitlin B. Houlton Kuntz

"All That IT Gibberish" – Part 2: Confidentiality and Data Security

Legal Update
03.02.2020

By Caitlin B. Houlton Kuntz and Nadja Baer

Part 1 of this article reviewed overlooked information technology (IT) and intellectual property (IP) provisions in bank vendor agreements. Part 2 focuses on the "big cheese" of any bank contract – confidentiality and data security.

A bank's data is precious, not only because of its value to both the bank and the bank's customers, but because it is heavily regulated by federal and state law. Not all vendor agreements are drafted with financial institutions in mind. While most vendors will at least nod at data privacy and security in their standard agreements, many vendors simply are not aware of the particular regulatory obligations that directly affect banks. Merely including standard confidentiality obligations and general compliance-with-applicable-laws provisions is not enough. Before entrusting a vendor with confidential data, it is critical that banks review and negotiate contractual rights and obligations with respect to data.

1. Understand the Exposure

When reviewing and negotiating data security provisions, take stock of what the relationship entails and what categories of data are in play. Will the vendor have access to or control over customer information? What about any sensitive financial data, confidential supervisory information, or personally identifiable information? Will the vendor have contact with customers? Does the vendor operate overseas or outsource any of its obligations to third parties? Answers to these questions will help establish the depth and breadth of appropriate data security provisions.

2. Definitions Matter

Terms like "Confidential Information," "Customer Data," and "Personal Information" must be properly defined. The use and disclosure of certain types of customer information is restricted by law (such as "nonpublic personal information" under the Gramm-Leach-Bliley Act (GLBA)), and all parties should clearly understand how certain data will be treated. Note, however, that simply using these regulatory definitions may not be sufficient, as they are generally geared toward consumer customer information. Banks should ensure their commercial customers' data is

covered by the same protections.

While protection of customer data is indeed crucial, don’t overlook the bank’s own confidential information. Business plans, financial data, information security plans, and other proprietary information should all be kept confidential, and the bank should have remedies for any security compromise or impermissible disclosure.

3. Data Ownership and Non-Disclosure

IP provisions typically address which party owns which aspects of the services, including both the data that is provided to the vendor and the data that is produced using the software. Banks should retain ownership of their input and output data (particularly customer data) and prohibit the vendor from using, selling, or otherwise transferring such data for purposes other than as specifically permitted by the contract. Disclosure should generally be limited to when necessary to provide the services covered by the contract (to subcontractors and service providers, for example), and such disclosure should be covered by suitable confidentiality agreements. Further, banks should look carefully at any language that allows the vendor to de-identify and aggregate the bank’s data.

Vendors typically include provisions protecting and restricting the disclosure of their own data. Since regulators will expect unrestricted access to information regarding the bank’s third parties, double-check such language to ensure the bank may share proprietary vendor information with its regulators.

4. Information Security Programs

Banks must maintain rigorous information security programs to protect their systems and data, and vendors who have access to sensitive data should do the same. Vendors who handle customer information or have access to the bank’s critical systems should give assurances that they will maintain reasonable information security programs consistent with regulatory requirements, including GLBA and the Interagency Guidelines Establishing Information Security Standards. Vendors who store or process payment card data should be compliant with the Payment Card Industry Data Security Standard (PCI-DSS). Beyond implementing such measures, vendors should regularly test and maintain them. Look for provisions requiring vendors to conduct regular security audits, provide copies of the resulting reports, and address any problems discovered.

5. Security Breaches – The Nightmare Scenario

For no industry is a security incident a bigger headache than for financial institutions. A laundry list of state and federal notification requirements, response protocols, and mitigation expectations can bring a bank’s operations to a grinding halt in the wake of a security breach. Because banks remain primarily liable to regulators and customers for security breaches within systems provided by vendors, ensuring

contracts address them properly is key.

First, define what constitutes a “security breach.” Ideally, it will include any situation in which a vendor knows, reasonably suspects, or has been threatened with the unauthorized disclosure of the bank’s confidential information. Next, make sure the vendor is required to notify the bank promptly in the event of a security breach and take steps necessary to mitigate any damage. Third, the vendor should agree to cooperate with the bank to meet any notice requirements to customers and regulators. Finally, the contract should clearly assign liability for costs.

Apportioning liability is important, as security breaches can become very expensive very quickly. Negotiate what expenses the vendor will cover (such as notification costs, regulatory fines, and credit monitoring expenses) and pay attention to any monetary caps on damages. Appropriate contractual remedies and insurance obligations should be negotiated based on the magnitude of the potential risk rather than the annual cost of the contract itself.

Since regulators can and will hold banks liable for issues caused by third parties, contracts should be carefully evaluated and negotiated to limit the bank’s exposure. Vendors who regularly work with banks are accustomed to these conversations, and refusal by a vendor to negotiate reasonable confidentiality and data security provisions is a significant red flag. Confidentiality and data security provisions can be tricky, but bankers should not overlook or be intimidated by complex technical jargon. As with the IT/IP provisions discussed in Part 1, putting the time and effort into reviewing and negotiating confidentiality and data security provisions before signing a contract can avoid stress and expense later.