GLBA Compliance Considerations in Technology Transactions
By Robert J. Scott

I am a technology attorney representing financial institutions in transactions with service providers. The Gramm-Leach-Bliley (GLB) Act is a federal law that requires financial institutions take steps to ensure the security and confidentiality of customer data. As part of its implementation of the GLB Act, the Federal Trade Commission (FTC) requires financial institutions under its jurisdiction to safeguard customer records and information. This requirement is known as the Safeguards Rule.

The Safeguards Rule applies to organizations that are significantly engaged in providing financial products or services to consumers, including check-cashing businesses, data processors, mortgage brokers, nonbank lenders, personal property or real estate appraisers, and retailers that issue credit cards to consumers.

According to the Safeguards Rule, financial institutions must develop a written information security plan that describes their program to protect customer information. All programs must be appropriate to the financial institution's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information at issue. Covered financial institutions must among other things, select appropriate service providers and require them (by contract) to implement the safeguards.

From a transactional perspective, the Safeguards rule requires due diligence to insure that all service providers are "appropriate." Once a service provider has been selected, appropriate contract language must be added in order to be in compliance with the Act.

Pursuant to Section 501(b) of GLBA, financial regulators have published the Interagency Guidelines for Establishing Information Security Standards and have established audit protocols to gauge compliance during routine audits.

Service Provider Definition

Under the regulations, a service provider is *any* party that is permitted access to a financial institution's customer information through the provision of services directly to the institution. Examples of service providers include a person or corporation that tests computer systems or processes customers' transactions on the institution's behalf, document-shredding firms, transactional Internet banking service providers, and computer network management firms.

Overseeing Service Providers

The Security Guidelines establish specific requirements that apply to a financial institution's contracts with service providers. An institution must:

- Exercise appropriate due diligence in selecting its service providers;
- Require its service providers by contract to implement appropriate measures designed to meet the objectives of the Security Guidelines; and
- Where indicated by its risk assessment, monitor its service providers to confirm that they have satisfied their obligations under the contract described above.

1256 Main Street, Suite 200 · Southlake, Texas 76092
p 214.999.0080 · f 214.999.0333
Scott & Scott, LLP
Website · Disclaimer

Sample Language for Monitoring and Oversight

Here is the language I like to use to make sure that the financial institution is in compliance with the requirement to oversee the service provider.

> *Use of Subcontractors. Vendor may use subcontractors in connection with this agreement provided that Vendor's use of subcontractors is in compliance with the requirements set forth in 501(b) of GLBA. Upon request Vendor must certify that its vendors and subcontractors are in compliance with GLBA.*
>
> *Oversight. Upon request, Vendor shall provide BANK with copies of audits, summaries of test results, or equivalent evaluations to confirm that Vendor is in compliance with its obligations under GLBA.*

Requiring Service Providers to Implement Appropriate Security Measures

The contract provisions in the Security Guidelines apply to *all* of a financial institution's service providers. After exercising due diligence in selecting a company, the institution must enter into and enforce a contract with the company that requires it to implement appropriate measures designed to implement the *objectives* of the Security Guidelines.

In particular, financial institutions must require their service providers by contract to

- Implement appropriate measures designed to protect against unauthorized access to or use of customer information maintained by the service provider that could result in substantial harm or inconvenience to any customer; and
- Properly dispose of customer information.

Sample Language for Safeguards Rule

I use this language to make sure that that the service provider is contractually bound to implement appropriate measures.

> *Compliance With Laws. Vendor represents and warrants that the Services will be performed consistent with all applicable laws, rules and regulations, and that it will promptly re-perform at its expense any Services that fail to meet that standard. Vendor acknowledges that BANK is subject to the GLB Act, Title V, ("GLBA") and that Vendor is considered a service provider under GLBA. During the term of this agreement, Vendor shall have, adequate administrative, technical, and physical safeguards designed to protect against unauthorized access to or use of customer information maintained by it or its subcontractors or vendors that could result in substantial harm or inconvenience to BANK or any customer, as set forth in GLBA to (i) ensure the security and confidentiality of such BANK Data; (ii) help protect against any anticipated or reasonably likely threats or hazards to the security or integrity of such BANK Data; (iii) help protect against unauthorized access to or use of such BANK Data; and (iv) ensure the proper disposal of BANK Data.*

1256 Main Street, Suite 200 · Southlake, Texas 76092
p 214.999.0080 · f 214.999.0333
Scott & Scott, LLP
Website · Disclaimer

Incident Response Rule

In addition, the Incident Response Guidance requires a service provider to take appropriate actions to address incidents of unauthorized access to the financial institution's customer information, including notification to the institution as soon as possible following any such incident.

Sample Language for Incident Response

Here is the sample language I like to use to use for the incident response rule.

> *Incident Response. Vendor will take appropriate actions to address incidents of unauthorized access to BANK's customer information, including notifying BANK as soon as possible following any such incident.*

When representing financial institutions in transactions with service providers, it is critically important to understand the regulatory framework and how it impacts the transaction. I rarely see vendor contracts that comply with these regulations. Failure to comply with the GLBA safeguards rules and contracting requirements with services providers can result in adverse audit findings by regulators and potentially increase liability for privacy and security claims for damages. If you are financial institution seeking counsel to assist with service provider contracts, please contact me to learn how we can help.

About the author Rob Scott:

Robert represents mid-market and large enterprise companies in software license transactions and disputes with major software publishers such as Adobe, IBM, Microsoft, Oracle and SAP. He has defended over 225 software audit matters initiated by software piracy trade groups such as the BSA and SIIA. He is counsel to some of the world's largest corporations on information technology matters including intellectual property licensing, risk management, data privacy, and outsourcing. Robert ensures that Scott & Scott, LLP continues its focus on cost-effective strategies that deliver positive results.

Get in touch: rjscott@scottandscottllp.com | 800.596.6176