Vendor Contracting and GLBA's Safeguards Rule

By Rob Scott
Scott & Scott LLP

I am a technology lawyer representing banks and other financial institutions in technology transactions. As you might imagine, many of my clients are investing heavily in security products and services. In some instances, they are considering cloud solutions to enhance their customers' experiences. Financial institutions are regulated by the Gramm, Leach, Bliley Act, ("GLBA") which is codified at 16 CFR 314. GLBA defines financial institutions as all business, regardless of size, that are significantly engaged in offering financial goods or services. GLBA includes both privacy and safeguard rules related to customer information. These rules require financial institutions to implement adequate administrative, procedural, and technical safeguards designed to safeguard customer information.

What is a service provider under GLBA Safeguard's Rule?

GLBA extends to the financial institution's vendors by operation of law if the vendor meets the definition of service provider. A service provider is defined as:

> Any party that is permitted access to a financial institution's customer information through the provision of services directly to the institution.

Given the complexity of hosted and cloud based services, it is sometimes difficult to determine if a vendor meets the service provider definition under GLBA. This is an important threshold issue in any transaction because GLBA has specific rules regarding vendor due diligence and required contract provisions for contracts with service providers.

What is customer information under GLBA Safeguard's Rule?

At the beginning of a new project, counsel should discuss the potential operational and legal risks of the proposed transaction. It is critical to understand where the data will reside and how it will be moved, shared, and stored. Counsel should keep probing until clear on the question of whether the proposed transaction involves customer information as that term is defined under GLBA 16 C.F.R. 313(n) which provides:

> (n)
> (1) Nonpublic personal information means:
> (i) Personally identifiable financial information; and
> (ii) Any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available.
>
> (2) Nonpublic personal information does not include:
> (i) Publicly available information, except as included on a list described in paragraph (n)(1)(ii) of this section; or
> (ii) Any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived without using any personally identifiable financial information that is not publicly available.
>
> (3) Examples of lists —
> (i) Nonpublic personal information includes any list of individuals' names and street addresses that is derived in whole or in part using personally identifiable financial information (that is not publicly available), such as account numbers.
> (ii) Nonpublic personal information does not include any list of individuals' names and addresses that contains only publicly available information, is not derived, in whole or in part, using personally identifiable financial information that is not publicly available, and is not disclosed in a manner that indicates that any of the individuals on the

list is a consumer of a financial institution.

I look to 313(n) for the definition of customer information even though it is in the GLBA Privacy Rule. The GLBA Safeguards Rule's definition of customer information is contained in 16 CFR 314.2 and reads as follows:

> *Customer information* means any record containing nonpublic personal information as defined in 16 CFR 313.3(n), about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of you or your affiliates.

Therefore, I have to understand whether the vendor will be permitted access to any record containing personally identifiable financial information or any list, description or grouping derived using personally identifiable financial information. If I conclude that that data in question includes personally identifiable financial information then I continue to the next line of questions.

What is permitted access under GLBA?

After determining whether or not customer information is at risk, counsel should evaluate the proposed architecture and service delivery options. These questions may include: How the vendor will deliver services? Where are the applications hosted? Who owns the hardware? To properly apply the GLBA safeguards rules, everyone should understand how the vendor will interact with customer data throughout the project life cycle. It is usually pretty easy to determine whether the vendor will be permitted access to customer data if they are hosting in the vendor's cloud. More difficult permission cases include service and support of on-premises applications where service providers are given access to customer data to trouble-shoot or resolve issues. I assume all vendors whose applications store customer information to be service providers under GLBA's safeguards rule unless I am convinced

otherwise during the client interview. Rarely, the client will present a use case involving an on-premises deployment of an application where the vendor never has access to the application. Most of the time, even when on-premises deployments are further evaluated, the vendor is a service provider because they are permitted access to the application during implementation or when performing maintenance and support. A vendor is not a service provider under GLBA merely because a compromise of the vendors system could lead to access to customer data. Accordingly, the GLBA safeguards rule is triggered only when access is given by permission, either through the contract or operationally.

Transactions between financial institutions and their technology services providers are often regulated by GLBA. Lawyers need to determine whether the transaction involves personally identifiable financial information and if so, whether the vendor will ever be permitted access to any records at any time. These two issues will determine whether the vendor is a service provider under GLBA’s Safeguards Rule. Once the determination has been made, GLBA imposes numerous additional requirements for both the service provider and financial institution.