Data Security Contract Clauses for Service Provider Arrangements (Pro-customer)

Dana B. Rosenfeld and Alysa Zeltzer Hutnik, Kelley Drye & Warren LLP

Sample clauses for use in a services agreement that involves the use, storage or other processing of personal information by the service provider. These clauses are drafted in favor of a customer, but aim to be reasonable. They may be incorporated into the services agreement or attached as a schedule to the agreement. These Standard Clauses have integrated notes with important explanations and drafting and negotiating tips.

Read this Before Using Document

As the outsourcing of business functions has become more popular, businesses are sharing increasing amounts of data, which is often highly confidential, with external service providers. Often, these service providers must use personal information supplied to them by their customers to provide the relevant services. This personal information may pertain to the customer’s employees and contractors, its own customers, business partners or other third parties.

The customer acting as a service recipient can face significant financial and reputational harm due to a security breach or the unauthorized use of shared personal information. In this case, both the customer and service provider must contend with a matrix of obligations governing the disclosure of personal information under federal and state laws and regulations, common law privacy principles and industry guidelines and standards (see Practice Note, US Privacy and Data Security Laws: Overview (http://us.practicallaw.com/6-501-4555)).

Some of these laws, including California and Massachusetts law, require that non-affiliated service providers contractually agree to take reasonable or appropriate measures to protect shared personal information (see Practice Note, US Privacy and Data Security Laws: Overview: State Laws (http://us.practicallaw.com/6-501-4555)).
Therefore, a customer must put in place appropriate contractual protections with each of its service providers having access to the customer’s personal information to:

- Specify the service provider’s standard of care and its obligations with respect to the treatment of personal information.
- Minimize the risks and liabilities associated with a service provider’s security breach or the unauthorized use of personal information.

**Scope of the Standard Clauses**

These sample clauses provide a general template to assist in preparing data security clauses for use in a services agreement that involves the use, storage or other processing of personal information, including highly-sensitive personal information, by a service provider on behalf of a customer. They are drafted from the perspective of the customer.

When drafting or negotiating data security clauses, it is important to consult with an information security or privacy lawyer. In particular, these clauses must be modified or supplemented as necessary to reflect

- **The particular facts and circumstances of the relevant transaction:** Not all of the clauses included in this document may be relevant or appropriate for a particular transaction. For example, the parties need to take into account:
  - The sensitivity of the personal information at issue.
  - The results of the customer’s due diligence of the service provider’s capability to comply with the customer’s data security requirements.
  - The parties’ individual written information security policies and other internal policies and procedures.

- **Any specific applicable legal requirements:** Specific laws, including the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH), the Fair Credit Reporting Act (FCRA) and the Children’s Online Privacy Protection Act (COPPA) may impose additional requirements on the parties. Companies subject to those laws should review the privacy and data security requirements of those statutes to ensure that their service provider agreements fully comply and that they comply with any additional obligations relating to the disclosure of personal information to a third party. For a model agreement between an entity subject to HIPAA’s privacy and security rules and its business associate, see [Standard Document, Business Associate Agreement](http://us.practicallaw.com/3-501-6706).

**Assumptions**

These standard terms and conditions are drafted on the following assumptions:

- Both the service provider and customer are US corporate entities and the agreement is governed by US laws.
- The transaction does not involve the cross-border sharing of personal information. If the transaction involves the cross-border sharing of personal information, the laws of the relevant foreign jurisdictions must be reviewed for compliance. For example, the transfer of personal data from the European Economic Area (EEA) to the US and other countries may require the inclusion of standard contractual clauses that further specify how the processing of personal data will be treated (see [Article, Solutions to the cross-border transfers of personal data from the EEA](http://us.practicallaw.com/3-385-6772)).
DATA SECURITY CONTRACT CLAUSES FOR SERVICE PROVIDER
ARRANGEMENTS (PRO-CUSTOMER)

1. DEFINITIONS.

Capitalize terms used herein shall have the meanings set forth in this Section [1].

**Definitions**

Certain terms are capitalized but not defined in these clauses because they will be defined elsewhere in the relevant services agreement (for example, Agreement, Customer, Service Provider, Governmental Authorities and Confidential Information). You should ensure they conform to the defined terms used in your agreement.

“Authorized Employees” means Service Provider’s employees who have a need to know or otherwise access Personal Information to enable Service Provider to perform its obligations under this Agreement.

**Authorized Employees**

The definition of “Authorized Employees” is limited to the service provider’s actual employees. These Standard Clauses permit the service provider to disclose personal information at a minimum to its employees in order to perform the relevant services.

The service provider may also seek or require the ability to disclose personal information to certain third parties in the ordinary course of business without the customer’s prior consent (see Drafting Note, Authorized Persons).

[“Authorized Persons” means (i) Authorized Employees; and (ii) Service Provider’s [contractors,] [agents,] [outsourcers] [and] [auditors] [as each is specified on Exhibit [EXHIBIT NUMBER] to this Agreement] who have a need to know or otherwise access Personal Information to enable Service Provider to perform its obligations under this Agreement, and who are bound in writing by confidentiality obligations sufficient to protect Personal Information in accordance with the terms and conditions of this Agreement.]
**Authorized Persons**

To avoid unnecessary security risks, the customer generally wants to limit the service provider’s ability to disclose personal information to third parties without the customer’s prior written consent. However, the service provider may seek or require flexibility to disclose personal information to certain third parties, such as its subcontractors or agents, without first seeking the customer’s permission.

If the particular arrangement merits a more permissive approach, this optional definition of “Authorized Persons” is provided to define those third parties permitted to receive personal information without the customer’s prior consent.

The customer should also consider using the bracketed language to have the service provider specifically identify the relevant third parties in an attached exhibit. Alternately, the types or categories of third parties can be more specifically described in the definition itself.

In considering these issues, the customer should also review and conform the language in Section 2(a) and Section 2(c)(iii).

**“Highly-Sensitive Personal Information”** means an (i) individual’s government-issued identification number (including social security number, driver’s license number or state-issued identified number); (ii) financial account number, credit card number, debit card number, credit report information, with or without any required security code, access code, personal identification number or password, that would permit access to an individual’s financial account; or (iii) biometric or health data.

**“Personal Information”** means information provided to Service Provider by or at the direction of Customer, or to which access was provided to Service Provider by or at the direction of Customer, in the course of Service Provider’s performance under this Agreement that: (i) identifies or can be used to identify an individual (including, without limitation, names, signatures, addresses, telephone numbers, e-mail addresses and other unique identifiers); or (ii) can be used to authenticate an individual (including, without limitation, employee identification numbers, government-issued identification numbers, passwords or PINs, financial account numbers, credit report information, biometric or health data, answers to security questions and other personal identifiers), in case of both subclauses (i) and (ii), including, without limitation, all Highly-Sensitive Personal Information. Customer’s business contact information is not by itself deemed to be Personal Information.

**Personal Information and Highly-Sensitive Personal Information**

The definition of personal information used in the various federal and state privacy and data security laws that regulate the use of personal information varies based on the focus and scope of the regulation. The definition of personal information in these clauses aims to be broadly drafted and may be more broadly defined than the relevant federal or state laws.

There is also no statutory definition for highly-sensitive personal information, but this term is commonly defined in service provider agreements to include certain types of personal information that might be more sensitive or pose greater risk if disclosed in an unauthorized manner, including:

- Social security numbers.
- Financial information.
- Medical information.
“Security Breach” means (i) any act or omission that materially compromises either the security, confidentiality or integrity of Personal Information or the physical, technical, administrative or organizational safeguards put in place by Service Provider ((or any Authorized Persons)) that relate to the protection of the security, confidentiality or integrity of Personal Information, or (ii) receipt of a complaint in relation to the privacy practices of Service Provider ((or any Authorized Persons)) or a breach or alleged breach of this Agreement relating to such privacy practices.

The customer would prefer to receive alerts as to any potential privacy-related compliance issue, not just an actual security breach. The optional language in subclause (ii) addresses this by including privacy-related complaints under the definition of “Security Breach”.

The service provider will likely push back on the inclusion of this language. If included as part of the definition, the service provider will be required to undertake a series of actions, from notification to remediation, on the receipt of a complaint (see Section 4). In response, the customer can consider adding a separate notification obligation for complaints to the agreement that is not part of this definition.

2. STANDARD OF CARE.

(a) Service Provider acknowledges and agrees that, in the course of its engagement by Customer, Service Provider may receive or have access to Personal Information. Service Provider shall comply with the terms and conditions set forth in this Agreement in its collection, receipt, transmission, storage, disposal, use and disclosure of such Personal Information and be responsible for the unauthorized collection, receipt, transmission, access, storage, disposal, use and disclosure of Personal Information under its control or in its possession by all [Authorized Employees/Authorized Persons]. [Service Provider shall be responsible for, and remain liable to, Customer for the actions and omissions of all Authorized Persons that are not Authorized Employees concerning the treatment of Personal Information as if they were Service Provider’s own actions and omissions].
Responsibility for Authorized Persons

To the extent that third parties are permitted to receive or have access to personal Information as “Authorized Persons” (see Authorized Persons), the bracketed language in the last sentence should be included to ensure that the service provider is responsible for the actions of the relevant third parties.

(b) [Personal Information is deemed to be Confidential Information of Customer and is not Confidential Information of Service Provider. In the event of a conflict or inconsistency between this Section and [the confidentiality/compliance with laws] sections of this Agreement, the terms and conditions set forth in this Section shall govern and control.]

Personal Information versus Confidential Information

The above provision gives the option to specify that customer’s personal information should also be treated as the customer’s confidential information under the agreement. However, the standard of care required for the protection of personal information may be higher than the general standard of care applicable to confidential information under the agreement or as may otherwise be required by law. Therefore, to avoid any conflict or inconsistency, the bracketed language also specifies that this provision should govern in the event of any conflict or inconsistency between this provision and the confidentiality or compliance with laws provisions of the agreement.

(c) In recognition of the foregoing, Service Provider agrees and covenants that it shall:

(i) keep and maintain all Personal Information in strict confidence, using such degree of care as is appropriate to avoid unauthorized access, use or disclosure;

(ii) use and disclose Personal Information solely and exclusively for the purposes for which the Personal Information, or access to it, is provided pursuant to the terms and conditions of this Agreement, and not use, sell, rent, transfer, distribute, or otherwise disclose or make available Personal Information for Service Provider’s own purposes or for the benefit of anyone other than Customer, in each case, without Customer’s prior written consent; and

(iii) not, directly or indirectly, disclose Personal Information to any person other than [its Authorized Employees/Authorized Persons] [including any subcontractors, agents, outsourcers or auditors] (an "Unauthorized Third Party”), without express written consent from Customer [unless and to the extent required by Government Authorities or as otherwise, to the extent expressly required, by applicable law, in which case, Service Provider shall (i) use best efforts to notify Customer before such disclosure or as soon thereafter as reasonably possible; (ii) be responsible for and remain liable to Customer for the actions and omissions of such Unauthorized Third Party concerning the treatment of such Personal Information as if they were Service Provider’s own actions and omissions; and (iii) require the Unauthorized Third Party that has access to Personal Information to execute a written agreement agreeing to comply with the terms and conditions of this Agreement [relating to the treatment of Personal Information]].
3. INFORMATION SECURITY.

(a) Service Provider represents and warrants that its collection, access, use, storage, disposal and disclosure of Personal Information does and will comply with all applicable federal [and], state[, and foreign] privacy and data protection laws, as well as all other applicable regulations and directives.

(b) Without limiting Service Provider's obligations under Section [3(a)], Service Provider shall implement administrative, physical and technical safeguards to protect Personal Information that are no less rigorous than accepted industry practices ([including/specifically] [the International Organization for Standardization's standards: ISO/IEC 27001:2005 – Information Security Management Systems – Requirements and ISO-IEC 27002:2005 – Code of Practice for International Security Management,] [the Information Technology Library (ITIL) standards,] [the Control Objectives for Information and related Technology (COBIT) standards] [or] [other applicable industry standards for information security]), and shall ensure that all such safeguards, including the manner in which Personal Information is collected, accessed, used, stored, processed, disposed of and disclosed, comply with applicable data protection and privacy laws, as well as the terms and conditions of this Agreement.
Compliance with IT Management Standards

Compliance with the various standards referenced in this paragraph may be time-consuming and expensive for the service provider. Therefore, the service provider may seek to limit its obligations to comply by such standards, if it has not already evaluated its practices or obtained the referenced certifications. When selecting the appropriate security standards for the transactions, the customer should take into account the service provider’s capabilities and its ability to provide appropriate assurances, as well as the overall nature of the transaction.

While this provision does not require the service provider evidence of its compliance with these standards, the customer can require the service provider to provide relevant audit reports in Section 5.

ISO/IEC 27001:2005 specifies the requirements that need to be met for International Organization for Standardization (ISO) certification. It is closely related to the code of practice in ISO/ICE 28002. Topics covered by these standards include:

- Identity and access management.
- Infrastructure and operations security.
- Vulnerability management.
- Business-continuity planning.
- Disaster-recovery planning.
- Training.

The Control Objectives for Information and related Technology (COBIT), created by the ISACA and the IT Governance Institute (ITGI), and the Information Technology Infrastructure Library (ITIL), created by the UK’s Office of Government Commerce, offer similar sets of best practices for information technology management.

(c) If, in the course of its engagement by Customer, Service Provider has access to or will collect, access, use, store, process, dispose of or disclose credit, debit or other payment cardholder information, Service Provider shall at all times remain in compliance with the Payment Card Industry Data Security Standard (“PCI DSS”) requirements, including remaining aware at all times of changes to the PCI DSS and promptly implementing all procedures and practices as may be necessary to remain in compliance with the PCI DSS, in each case, at Service Provider’s sole cost and expense.

Compliance with Payment Card Industry Data Security Standard (PCI DSS)

If the customer is sharing credit card payment data with the service provider, the customer should require that the service provider specifically agree to comply with the data security standards set out by the payment card industry (see Practice Note, US Privacy and Data Security Law: Overview: Payment Card Industry Data Security Standard (PCI DSS) (http://us.practicallaw.com/6-501-4555)). It is also reasonable for the customer to require the service provider to monitor relevant changes in the PCI DSS and make any required changes to comply with such changes.

(d) At a minimum, Service Provider’s safeguards for the protection of Personal Information shall include: (i) limiting access of Personal Information to [Authorized Employees/Authorized Persons]; (ii) securing business facilities, data centers, paper files, servers, back-up systems and computing equipment, including, but not limited
to, all mobile devices and other equipment with information storage capability; (iii) implementing network, device
application, database and platform security; (iv) securing information transmission, storage and disposal; (v)
implementing authentication and access controls within media, applications, operating systems and equipment;
(vi) encrypting Highly-Sensitive Personal Information stored on any mobile media; (vii) encrypting Highly-Sensitive
Personal Information transmitted over public or wireless networks; (viii) strictly segregating Personal Information
from information of Service Provider or its other customers so that Personal Information is not commingled with
any other types of information; (ix) implementing appropriate personnel security and integrity procedures and
practices, including, but not limited to, conducting background checks consistent with applicable law; and (x)
providing appropriate privacy and information security training to Service Provider’s employees.

Minimum Security Safeguards

The customer should contractually obligate the service provider to implement and maintain
specific minimum safeguards for the treatment of personal information, particularly if the service
provider is handling highly-sensitive personal information.

If the service provider objects to this provision, the customer can point to California’s and
Massachusetts’ data security regulations (see Practice Note, US Privacy and Data Security Laws:
Overview; California Laws (http://us.practicallaw.com/6-501-4555) and Massachusetts Data
Security Regulation (http://us.practicallaw.com/6-501-4555)) which require that the service
provider agree to implement reasonable or appropriate safeguards when entering into service
provider agreements. The customer can also point to similar data security standards set out
by the Federal Trade Commission and state attorneys general in bringing enforcement actions
for violations of Section 5 of the Federal Trade Commission Act or similar state laws prohibiting
unfair or deceptive business practices.

Where encryption of highly-sensitive personal information is required, the customer should
consider specifying the relevant encryption standard. Current examples of encryption standards
include National Institute of Standards and Technology’s (NIST) Federal Information Processing
Standards (FIPS) 140-2 (Security Requirements for Cryptographic Modules) and FIPS-197.

(e) During the term of each Authorized Employee’s employment by Service Provider, Service Provider shall
at all times cause such Authorized Employees to abide strictly by Service Provider’s obligations under
this Agreement [and Service Provider’s standard policies and procedures, a copy of which [have been
provided to Customer/are attached as Exhibit [EXHIBIT NUMBER] to this Agreement]]. [Service Provider
further agrees that it shall maintain a disciplinary process to address any unauthorized access, use or
disclosure of Personal Information by any of Service Provider’s officers, partners, principals, employees,
agents or contractors]. [Upon Customer’s written request, Service Provider shall promptly identify for
Customer in writing all Authorized Employees as of the date of such request.]

Oversight of Authorized Employees

This provision requires the service provider to ensure its employees’ compliance with the terms
and conditions of the agreement. It includes additional language requiring the service provider to
agree to maintain a disciplinary process to address any unauthorized use or disclosure.

The provision also includes optional language requiring the service provider to identify all
authorized employees in writing. The customer should decide if this requirement is appropriate
for the particular transaction.
(f) Upon Customer's written request, Service Provider shall provide Customer with a network diagram that outlines Service Provider's information technology network infrastructure and all equipment used in relation to fulfilling of its obligations under this Agreement, including, without limitation: (i) connectivity to Customer and all third parties who may access Service Provider's network to the extent the network contains Personal Information; (ii) all network connections including remote access services and wireless connectivity; (iii) all access control devices (for example, firewall, packet filters, intrusion detection and access-list routers); (iv) all back-up or redundant servers; and (v) permitted access through each network connection.

**IT Network Infrastructure Diagram**

This optional provision requires the service provider to deliver a detailed network infrastructure diagram. The customer should consider whether the particular transaction requires it to review these details regarding the service provider’s technical environment.

This can also be investigated as part of the customer’s due diligence. In this case, the customer can alternatively require the service provider to covenant that the disclosed controls and back-up systems will remain place while the service provider is in possession of or has access to the customer’s personal information.

### 4. SECURITY BREACH PROCEDURES.

**Security Breach Procedures**

The following security breach procedure provisions are not expressly required under US law to be in an agreement relating to the provision of personal information. However, it is strongly recommended that the customer include these provisions so that the service provider is contractually obligated to notify the customer and take other actions in the event of a security breach involving personal information.

(a) Service Provider shall:

(i) provide Customer with the name and contact information for an employee of Service Provider who shall serve as Customer's primary security contact and shall be available to assist Customer twenty-four (24) hours per day, seven (7) days per week as a contact in resolving obligations associated with a Security Breach;

(ii) notify Customer of a Security Breach as soon as practicable, but no later than [twenty-four (24)] hours after Service Provider becomes aware of it; and

(iii) notify Customer of any Security Breaches by [telephone at the following number: [TELEPHONE NUMBER]/e-mailing Customer with a read receipt at [E-MAIL ADDRESSES]] and with a copy by e-mail to Service Provider’s primary business contact within Customer.

(b) Immediately following Service Provider’s notification to Customer of a Security Breach, the parties shall coordinate with each other to investigate the Security Breach. Service Provider agrees to [fully/reasonably] cooperate with Customer in Customer's handling of the matter, including, without limitation: (i) assisting with any investigation; (ii) providing Customer with physical access to the facilities and operations affected; (iii) facilitating interviews with Service Provider’s employees and others involved in the matter; and (iv) making available all relevant records, logs, files, data reporting and other materials required to comply with applicable law, regulation, industry standards or as otherwise (reasonably) required by Customer.
Immediately following Service Provider’s notification to Customer of a Security Breach, the parties shall coordinate with each other to investigate the Security Breach in accordance with Service Provider’s standard policies and procedures, a copy of which [has been provided to Customer/is attached as Exhibit [EXHIBIT NUMBER] to this Agreement.]

(c) Service Provider shall [take reasonable steps to/use best efforts to] immediately remedy any Security Breach and prevent any further Security Breach at Service Provider’s expense in accordance with applicable privacy rights, laws, regulations and standards. [Service Provider shall reimburse Customer for actual [reasonable] costs incurred by Customer in responding to, and mitigating damages caused by, any Security Breach, including all costs of notice and/or remediation pursuant to Section 4(d).]

**Cooperation in the Event of Security Breach**

The customer typically wants the service provider to cooperate fully and promptly in the investigation of any security breach. Most importantly, the customer’s investigation (including identifying what happened and how many individuals were affected) may be delayed if the service provider refuses to provide the customer with necessary information or copies of relevant documents.

Two alternative sample clauses are provided above. The first alternative requires the service provider to cooperate with the customer and outlines the service provider’s related obligations.

The parties can consider using the second alternative if the service provider has standard policies and practices for responding to security breaches that have been or can be provided to the customer. The customer should ensure that the service provider’s description of its policies and practices is appropriate and sufficient for the relevant transaction.

**Expenses of Remediation for a Security Breach**

The bracketed language in the second sentence of the above clause requires the service provider to directly reimburse the customer for the costs it incurs if the service provider suffers a security breach. This is important because the indemnification obligations of the agreement may not cover all or some of the costs the customer may incur in responding to a data breach. The clause requires the service provider to be responsible for related costs in the first instance (that is, before any claims for indemnification the customer may have). This may reduce the customer’s overall expenses and help to avoid any potential ambiguity concerning the costs of responding to and mitigating a security breach.

A service provider will want to limit its liability and, therefore, is likely to push back on the inclusion of the second sentence of the above clause or seek to make it subject to a liability cap.

If the Service Provider objects to the second sentence of the above clause, and the type of personal information shared with or accessed by the service provider includes highly-sensitive personal information (such as social security numbers, payment card information or health information), the customer can propose the following alternative provision:

(Service Provider shall reimburse Customer for actual [reasonable] costs incurred in providing individuals affected by a Security Breach with notice of the breach, reissued payment cards, complimentary access for one (1) year credit monitoring services, credit protection services, credit fraud alerts and/or similar services, which Customer [in its sole
(d) [Service Provider agrees that it shall not inform any third party of any Security Breach without first obtaining Customer’s prior written consent, other than to inform a complainant that the matter has been forwarded to Customer’s legal counsel. Further, Service Provider agrees that Customer shall have the sole right to determine: (i) whether notice of the Security Breach is to be provided to any individuals, regulators, law enforcement agencies, consumer reporting agencies or others as required by law or regulation, or otherwise in Customer’s discretion; and (ii) the contents of such notice, whether any type of remediation may be offered to affected persons, and the nature and extent of any such remediation.]

Disclosure of Breach to Third Parties

Ideally, the customer wants control of all public announcements relating to any security breach, as well as the substance of these announcements. However, this clause is optional and the customer should determine whether it is appropriate or necessary for the particular transaction.

A service provider may assert that in the event of a security breach it has a legal requirement to notify third parties. For example, a service provider typically will want an exception covering criminal activity. Below is a modified version of the above clause permitting the service provider to make disclosures in that instance:

[Service Provider reserves the right, in its sole discretion, to report criminal acts relating to the use and disclosure of Personal Information to applicable Government Authorities and shall notify Customer as soon as practicable that such reporting has occurred. With respect to instances in which Service Provider is considering notifying Government Authorities concerning civil, but not criminal, acts, Service Provider shall notify Customer in writing and consult with Customer prior to making any such notification. The parties shall immediately endeavor in good faith to reach agreement on the need and nature of such notification. If such agreement cannot be reached within [seventy-two (72)] hours after Service Provider has provided Customer with written notice, Service Provider shall have the right to inform Government Authorities solely to the extent required by applicable law.]

(e) Service Provider agrees to [fully/reasonably] cooperate [at its own expense] with Customer in any litigation or other formal action deemed [reasonably] necessary by Customer to protect its rights relating to the use, disclosure, protection and maintenance of Personal Information.
(f) [In the event of any Security Breach, Service Provider shall promptly use its [reasonable/best] efforts to prevent a recurrence of any such Security Breach.]

Prevention of Future Breach

While this provision is optional, the customer should ensure that following a security breach, the service provider seeks to avoid any future incidents.

5. OVERSIGHT OF SECURITY COMPLIANCE.

Oversight of Security Compliance

This section includes three alternative provisions for the customer’s oversight of the service provider’s use and maintenance of personal information shared during the course of the agreement.

At a minimum, the customer should include the third alternative (see Drafting Note: Security Questionnaire), as it provides the customer with a baseline contractual right to some form of express oversight and requires the service provider’s cooperation. The first and second alternatives should also be considered for inclusion if they are appropriate for the particular transaction, but are not legally required if the customer is performing reasonable oversight and monitoring of the service provider’s security practices.

[Upon Customer’s [written] request, to confirm Service Provider’s compliance with this Agreement, as well as any applicable laws, regulations and industry standards, Service Provider grants Customer or, upon Customer’s election, a third party on Customer’s behalf, permission to perform an assessment, audit, examination or review of all controls in Service Provider’s physical and/or technical environment in relation to all Personal Information being handled and/or services being provided to Customer pursuant to this Agreement. Service Provider shall fully cooperate with such assessment by providing access to knowledgeable personnel, physical premises, documentation, infrastructure and application software that processes, stores or transports Personal Information for Customer pursuant to this Agreement. In addition, upon Customer’s [written] request, Service Provider shall provide Customer with the results of any audit by or on behalf of Service Provider performed that assesses the effectiveness of Service Provider’s information security program as relevant to the security and confidentiality of Personal Information shared during the course of this Agreement.]

Customer Audits

This provision grants the customer the right to conduct or oversee an audit of the service provider’s facilities and practices. If the service provider will have access to highly-sensitive personal information, it is strongly recommended that the customer include this provision.

To make this provision more appealing to the service provider, the customer can limit its right to conduct an audit to once a year, unless there has been a security breach or complaint relating to the service provider’s privacy and security practices.
OR

[At least [once] per year, Service Provider shall conduct site audits of the information technology and information security controls for all facilities used in complying with its obligations under this Agreement, including, but not limited to, obtaining a network-level vulnerability assessment performed by a recognized third-party audit firm based on the recognized industry best practices. Upon Customer’s written request, Service Provider shall make available to Customer for review all of the following, as applicable: Service Provider’s latest Payment Card Industry (PCI) Compliance Report, WebTrust, Systrust, and Statement on Standards for Attestation Engagements (SSAE) No. 16 audit reports for Reporting on Controls at a Service Organization and any reports relating to its ISO/IEC 27001 certification. [Customer shall treat such audit reports as Service Provider’s Confidential Information under this Agreement.] Any exceptions noted on the SSAE report or other audit reports will be promptly addressed with the development and implementation of a corrective action plan by service provider’s management.]

Auditing by Service Provider

If the service provider performs audits of its own compliance with accounting or industry standards, including SSAE 16 audits or those of a similar nature, the customer can include this clause instead of or in addition the first alternative.

For more information regarding SSAE 16 type audits and the relationship of such audits to public company obligations under Section 404 of the Sarbanes-Oxley Act of 2002, see Practice Note: Due Diligence in Outsourcing Transactions: Financial Reporting (http://us.practicallaw.com/6-501-4225). SSAE 16 replaces SAS 70 concerning service auditor reports for periods ending on and after June 15, 2011. For periods before June 15, 2011, management of a public company customer may still rely on a Type II SAS 70 report from the auditor of the service provider.

OR

[Upon the Customer’s written request, to confirm compliance with this Agreement, as well as any applicable laws and industry standards, Service Provider shall promptly and accurately complete a written information security questionnaire provided by Customer or a third party on the Customer’s behalf regarding Service Provider’s business practices and information technology environment in relation to all Personal Information being handled and/or services being provided by Service Provider to Customer pursuant to this Agreement. Service Provider shall fully cooperate with such inquiries. [Customer shall treat the information provided by Service Provider in the security questionnaire as Service Provider’s Confidential Information.]]

Security Questionnaire

At a minimum, the customer should include the above provision in this section, requiring the service provider to complete a security questionnaire. If appropriate, this provision can also used in addition to the first two alternatives.

To make this provision more appealing to the service provider, the customer can limit its right to submit a questionnaire to once a year, unless there has been a security breach or complaint relating to the service provider’s privacy and security practices. Alternatively, the customer can require the service provider to complete the questionnaire before the agreement is entered into and attach the questionnaire as an exhibit to the agreement. The customer can then require the service provider to give a representation and warranty that it is in compliance with the controls set out in the questionnaire and a covenant that it will remain in compliance for the duration of the agreement.
6. RETURN OR DESTRUCTION OF PERSONAL INFORMATION.

At any time during the term of this Agreement at the Customer’s request or upon the termination or expiration of this Agreement for any reason, Service Provider shall, and shall instruct all Authorized Persons to, promptly return to the Customer all copies, whether in written, electronic or other form or media, of Personal Information in its possession or the possession of such Authorized Persons, or securely dispose of all such copies, and certify in writing to the Customer that such Personal Information has been returned to Customer or disposed of securely. Service Provider shall comply with all directions provided by Customer with respect to the return or disposal of Personal Information.

Return or Destruction of Personal Information

To reduce the risks associated with the ongoing misuse use of personal information, the customer should require the service provider to return or destroy any personal information in its possession at any time promptly upon the customer’s request. The customer should also require the service provider to return or destroy personal information automatically upon any termination or expiration of the agreement (and not solely on the customer’s request). In each case, the service provider must also ensure the compliance of any authorized persons that possess personal information.

Alternatively, the customer can incorporate these obligations into the confidentiality provisions of the agreement. In that case, the customer should take into account any distinctions required for the treatment of personal information, as opposed to other confidential information.

The service provider may seek the right to retain personal information for legal compliance purposes or because it may be embedded in its electronic and offline files as part of its systematic back-up and archiving procedures. The customer should carefully consider whether these exceptions are appropriate for the transaction. If agreed on by the customer, any exceptions should state that the service provider will not use the retained information for any purposes and will otherwise continue to be bound by its obligations under the agreement.

Ideally, from the customer’s perspective, the service provider should be obligated to return all personal information on request. However, it is often impractical for the service provider to track and compile all the personal information to be returned. Therefore, as an alternative, the above provision permits the service provider to securely dispose of the information, so long as it certifies the destruction in writing.

At a minimum, the service provider should be obligated to promptly return or destroy the personal information in its possession, as it is usually unrealistic to expect a recipient to immediately return or destroy this information. The customer may instead insert a specific deadline (such as five or ten business days) for the service provider to comply.

7. EQUITABLE RELIEF.

Service Provider acknowledges that any breach of its covenants or obligations set forth in [this Section/SECTION NUMBER] or the Service Provider’s standard policies and procedures, a copy of which [have been provided to Customer/are attached as Exhibit [EXHIBIT NUMBER] to this Agreement] may cause Customer irreparable harm for which monetary damages would not be adequate compensation and agrees that, in the event of such breach or threatened breach, Customer is entitled to seek equitable relief, including a restraining order, injunctive relief, specific performance and any other relief that may be available from any court, in addition to any other remedy to which Customer may be entitled at law or in equity. Such remedies shall not be deemed to be exclusive but shall be in addition to all other remedies available at law or in equity, subject to any express exclusions or limitations in this Agreement to the contrary.
8. MATERIAL BREACH.

Service Provider’s failure to comply with any of the provisions of [this Section/SECTION NUMBER] is a material breach of this Agreement. In such event, Customer may terminate the Agreement effective immediately upon written notice to the Service Provider without further liability or obligation to Customer.

9. INDEMNIFICATION.

Service Provider shall defend, indemnify and hold harmless Customer, [and Customer’s [parent company] and [its/their] subsidiaries, affiliates, and [its/their] respective officers, directors, employees, agents, successors and permitted assigns] (each, a “Customer Indemnitee”) from and against all losses, damages, liabilities, deficiencies, actions, judgments, interest, awards, penalties, fines, costs or expenses of whatever kind, including reasonable attorneys’ fees, the cost of enforcing any right to indemnification hereunder and the cost of pursuing any insurance providers, arising out of or resulting from any third-party claim against any Customer Indemnitee arising out of or resulting from Service Provider’s failure to comply with any of its obligations under [this Section/SECTION NUMBER].
**Indemnification**

Indemnities, which allocate the risk of loss between the parties, are often heavily negotiated and the scope of the indemnity will in some cases depend on the type of transaction and bargaining power of the respective parties.

This indemnification provision relates specifically to the service provider’s failure to comply with its data security obligations, but alternatively can be incorporated into a separate, comprehensive indemnification clause in the agreement.

Wherever the indemnity is located, the parties should also ensure that the indemnification clause sets out the parties agreement concerning:

- Who controls the defense and the customer’s ability to participate if the service provider controls the defense.
- Whether the service provider is required to get the customer’s written consent before settling any claims.

**Customer**

The customer will want a broad indemnification from the service provider for third-party claims brought against it arising out of or related to the service provider’s failure to comply with its data security obligations. The customer should ensure that this indemnification provision does not conflict with any other indemnification provisions in the agreement.

The customer should also carefully review any provisions limiting the service provider’s liability, including any exclusions of consequential damages or caps on overall monetary liability, and consider excluding from these limitations both the service provider’s indemnification obligations in this section and breaches of the data security provisions. The customer should also consider if the indemnity needs to be extended to any third parties and tailor the bracketed language in the first sentence accordingly.

The customer should also consider whether it is appropriate to require the service provider to maintain insurance specifically covering data security breaches, in which case, the customer should include additional provisions in the contract relating to such insurance.

**Service Provider**

The service provider will want to limit the scope of any indemnification provision. At a minimum, the service provider will want to quantify its liability by making its indemnification obligations subject to a cap on the overall amount of damages. It may also seek to limit its liability to instances of gross negligence or willful misconduct. The customer should carefully consider any limitations on the scope of the service provider’s indemnification obligations, especially if the service provider is handling highly-sensitive personal information.