This sample addendum is provided as-is and is for example only. The sample addendum is provided without any representations or warranties, express or implied.

It is not intended as legal advice. It should not merely be duplicated without consideration of your particular situation.

It is not intended to cover each and every vendor relationship, nor can it anticipate specific needs.

**\INFORMATION SECURITY ADDENDUM TO**

**[MASTER SERVICES AGREEMENT]**

This Information Security Addendum is hereby incorporated by reference into the [INSERT AGREEMENT NAME] dated [INSERT DATE] (the "Agreement") between [INSERT VENDOR NAME] ("Company") and [INSERT LAW FIRM NAME] and its direct and indirect subsidiaries ("Customer") and shall be considered a part of the Agreement. In addition to the mutual promises and obligations set forth in the Agreement, Company agrees to the following provisions

1. Company has and will maintain a comprehensive, written Information Security Program that complies with all applicable laws and regulations and that is designed to (a) insure the security, privacy and confidentiality of Customer Information, (b) protect against any reasonably anticipated threats or hazards to the security or integrity of Customer Information, and (c) protect against unauthorized access to, use, deletion, or modification of Customer Information.
2. Company has designated one or more specifically named employees to be responsible for the administration of its Information Security Program;
3. Company has and will maintain a process for identifying, assessing, and mitigating the risks to Customer Information in each relevant area of Company's operations and evaluating the effectiveness of the safeguards for controlling these risks.
4. Company regularly monitors, tests, and updates its Information Security Program.
5. Company will restrict access to Customer Information only to those employees, agents, or subcontractors who have a need to know the information to perform their jobs (each an *“*Authorized Person" as defined below).
6. Company shall, at its own expense, report immediately to Customer any actual or suspected Breach of the confidentiality or security of any Customer Information (a "Breach" as defined below), along with any information reasonably requested by Customer to understand or remediate the Breach, including, but not limited to, the name and contact information for an employee of Company, who shall serve as Company's primary security contact and who will cooperate fully and assist Customer in resolving any Breach and determining the nature and root cause of the Breach. Notices shall be given to:

**[INSERT CONTACT INFORMATION**

1. Company shall, at its own expense, take reasonable steps and use best efforts to immediately remedy any Breach and prevent any future Breaches. Company shall reimburse Customer for actual costs incurred by Customer in responding to, and mitigating damages caused by, any Breach, including all costs of notice and/or remediation deemed necessary by Customer to comply with applicable laws, contractual obligations and client demands; and shall allow Customer to solely control the notification of Customer clients, employees, or individuals affected by such Breach. Company shall not notify or discuss any incident or Breach without Customer's prior written consent. If Customer determines that the Agreement must be modified as a result of a Breach, the parties shall negotiate in good faith to make such modifications. If the Parties cannot agree on the terms of the modification, Customer shall be entitled to terminate the contract without penalty or cost.
2. Company will allow Customer to review and assess Company's information security program. Company agrees to make reasonable changes to its information security program to ensure it is capable of maintaining safeguards that are appropriate for the Customer Information at issue. Customer will be allowed to conduct audits of the comprehensive information security program once annually or to substitute a questionnaire to be promptly completed by company. Company will provide Customer with notice of the results of any security audits or reviews of its systems that reveal a risk that is likely to adversely impact Customer or Customer Information, and will keep Customer timely informed of its remediation efforts.
3. At Customer's request, Company will securely destroy or return all Customer Information in its possession and certify to Customer in writing that Company has done so. If Company destroys Customer Information rather than return it, Company will use destruction methods that are in compliance with all applicable state and federal laws and regulations including www.ftc.gov/os/2004/11/041118disposalfrn.pdf.
4. Before using a third party to provide services to Customer, Company will first obtain Customer's consent in writing and Company will require those third parties to agree in writing to provide the same safeguards for Customer Information as set forth in this Addendum.
5. Company will perform background checks of its employees that will have access to Customer Information, including a review of their references, employment eligibility, education, and criminal background to ensure they do not pose a risk to the security of Customer Information or Customer employees. Company will provide, upon request, a copy of its background check requirements for Customer's review and approval.
6. Company will safeguard information or items Customer gives Company in order to allow Company to access Customer Information, its computer networks, or its premises or those of other service providers or its clients, including keycards, codes, usernames, passwords, keys, badges, etc., as well as information that, if disclosed, would compromise the security of Customer Information, such as the designs of Customer's networks, information controls, or design of its computer systems.
7. Company has or will implement the following safeguards for systems that process, store or transmit Customer information:
	1. Identity and Access Management;
	2. Complex passwords that must be changed on a regular basis;
	3. Encryption of Customer Confidential Information, Customer Personal Information, and Customer Client Information if it is transmitted over public or wireless networks (e.g., via email, ftp, Internet, etc.);
	4. Encryption of portable media, laptops, desktops, smartphones, mobile devices, and new technologies that store Customer Information;
	5. Two-factor authentication for remote access to Company's networks;
	6. Upon hire and annually thereafter, training of all employees, (including any agents, and subcontractors with access to Customer Information) about their obligations to implement the Company's Information Security Program;
	7. Disciplinary measures for employees who violate Company's Information Security Program;
	8. Preventing terminated employees from accessing Customer information;
	9. Appropriately configured and updated firewall, antivirus, and spyware software;
	10. Prompt application of vendor-recommended security patches and updates to systems and other applications to avoid any adverse impact to Customer's systems or Customer Information; and
	11. Intrusion Detection or Prevention Systems with appropriate logging and alerts to monitor access controls and to assure data integrity and confidentiality.
	12. Separation of Duties
	13. Infrastructure and Physical Security
	14. Business Continuity Planning
	15. Disaster Recovery Planning

**Definitions**

1. **"Authorized Persons"** means Company's employees, contractors, agents, outsourcers, and auditors, who have a need to know or otherwise have access to Personal Information to enable Company to perform its obligations under this Addendum, and who are bound in writing by confidentiality obligations sufficient to protect Personal Information in accordance with the terms and conditions of this Addendum.
2. **"Breach"** means any act or omission that compromises either the security, confidentiality or integrity of Customer Information or the physical, technical, administrative or organizational safeguards put in place by Company or Authorized Persons that relate to the protection of the security, confidentiality or integrity of Personal Information or the receipt of a complaint in relation to the privacy or security practices of the Company or a breach or alleged breach of this Addendum relating to such privacy or security practices.
3. **"Customer Information"** means:
	1. Personal Information;
	2. Customer Client Information;
	3. Customer Confidential Information
4. **“Customer Confidential Information"** means:
	1. Non-public business information that a reasonable person would understand is confidential; and
	2. Any information defined as "Confidential" by the Agreement to which this Addendum is attached.
5. **"Personal Information"** means any information relating to an identified or identifiable individual. This includes, but is not limited to, name, postal address, email address, telephone number, date of birth, government-issued identification number including Social Security number, driver's license number or passport number, credit report information, financial account number including credit or debit card number with or without passwords, personal identification numbers, or other identifiers used to authenticate an individual, biometric, genetic, health or medical information, or any other unique identifier, regardless of whether it applies to such individual that is a Customer client, employee, vendor, or any other relationship to Customer.
6. **"Customer Client Information"** means any information relating to Customer's representation of its clients. This includes, but is not limited to the client's name, the fact they are a client of Customer, information provided to Customer by a client, the advice given to clients, etc.

**[INSERT VENDOR LEGAL NAME]**

By:

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Title:

Date:

**[INSERT LAW FIRM NAME]**

By:

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Title:

Date: