APPENDIX F – OUTSIDE COUNSEL INFORMATION SECURITY ADDENDUM

This Outside Counsel Information Security Addendum ("Security Addendum") sets forth the minimum information security requirements the firm must adopt to protect the confidentiality, integrity, and availability of all information processed under the Guidelines.

The following terms, as used herein, have the meanings set forth below.

1. DEFINITIONS

1.1 **"Liberty/Customer Information"** is defined as set forth in Section X. A (Data Protection and Privacy) of these Guidelines.

1.2 **"Critical Vulnerability"** means any vulnerability that compromises, or has the potential to compromise the confidentiality, integrity, availability or security of Liberty/Customer Information.

1.3 **"Information Assets"** means any valuable and important information or data that an organization possesses. These assets can include but are not limited to intellectual property, customer information, financial records, trade secrets, research and development data, employee records, and any other sensitive or confidential information that is critical to the operations and success of the organization.

1.4 **"Security Incident"** means any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Liberty/Customer Information processed or otherwise handled by the firm or the firm's sub-contractors.

1.5 **"Sub-contractor(s)"** means any party engaged by the firm that processes or handles Liberty/Customer Information, including the firm's affiliates or other companies within the firm's group carrying out activities in respect of Liberty/Customer Information.

1.6 **"Firm"** as used herein, shall be deemed to include the law firm, and, where applicable, the law firm's personnel and sub-contractors.

2. MINIMUM SECURITY REQUIREMENTS

2.1. Information Security Program Governance

2.1.1. **Written Information Security Program.** Firm shall maintain a formally documented information security program, with up-to-date policies and procedures for the administration of information security, including compliance with industry standards for information security, such as ISO/IEC 27001, NIST, and GDPR, throughout its organization.

2.1.2. **Information Security Policies.** Firm shall maintain up-to-date information security policies that are reviewed and approved no less than annually.

2.1.3. **Security Awareness and Training.** Firm shall maintain a comprehensive security training and awareness procedure for all employees and contractors who have access to Liberty/Customer Information or Liberty's information systems. Such procedures should include but not be limited to information security best practices, handling of sensitive data, and awareness of potential cyber security threats, and be carried out at least annually.

2.2. Access and Authentication

2.2.1. Account Management. Firm shall maintain formally documented procedures for creation, review, and deactivation of user accounts.

2.2.2. Network and Remote Access. Firm is expected to utilize multi-factor authentication for all connections, including both internal network (in-office, wired connections) and remote access communications.

2.2.3. Privileged Access. Firm shall utilize multi-factor authentication for access all administrative accounts and service accounts that prohibit interactive login.

2.2.4. Least Privilege. Firm shall limit access to information assets containing Liberty/Customer Information to authorized users to fulfill their duties on a need-to-use basis and following the least privilege principle.

2.3. Asset and Data Management

2.3.1. Asset Lifecycle. Firm shall maintain and follow industry standard asset management procedures that appropriately inventories, classifies, and controls hardware and software assets throughout their life cycle.

2.3.2. Acceptable Use. Firm shall formally document and implement rules for acceptable use outlining the expectations and constraints for employees and users regarding the utilization of Law Firm-provided technology, network resources, internet access, and data assets.

2.3.3. Portable Assets. If Firm allows employee access to Liberty/Customer Information from a portable device (e.g., USB, external hard drive, mobile devices, etc.), Law Firm shall maintain a formally documented policy and maintain a solution to ensure proper access authentication, encryption controls, and remote erasure.

2.4. Data Protection and Destruction

2.4.1. Data Protection. Firm shall ensure data classification, retention, and destruction policies, standards, and procedures based on industry standards have been established, are maintained, and are enforced appropriately.

2.4.2. Data Destruction. Liberty reserves the right to request the Firm provide evidence/certification of destruction of Liberty/Customer Information in the form of a certificate.

2.4.3 Consistency with Document Retention. These Minimum Security Requirements are in addition to document retention requirements set forth in the Guidelines.

2.5. Encryption Management

2.5.1. Encryption. Firm shall ensure encryption management policies, standards, and procedures based on industry standards have been established, are maintained, and are enforced appropriately.

2.5.2. Encryption of data-in-transit. Firm shall adhere to industry best practices for encryption in-transit for transferring Liberty/Customer Information across the public internet.

2.5.3. Encryption of data-at-rest. Firm shall enforce encryption at rest at locations where Liberty/Customer Information can and will be stored (inclusive of email server level, local storage on end user devices, file storage sites/other SaaS offerings, etc.) with industry standard encryption and/or equivalent cryptographic keys and algorithms.

2.6. Incident Response and Recovery

2.6.1. Incident Response Plan. Firm shall maintain a formally documented Incident Response Plan with procedures to investigate, contain, and mitigate cybersecurity events. Incident Response Plan shall be reviewed at least annually and tested at appropriate intervals by Law Firm.

2.6.2. Business Continuity and Disaster Recovery. Firm shall maintain a formally documented Business Continuity and Disaster Recovery Plan ("BCDRP") with procedures to minimize the impact of events, whether related to technology or operational failures, which may affect the firm's ability to provide services. BCDRP shall be reviewed annually and tested at appropriate intervals by Law Firm.

2.7. Network and Systems Security

2.7.1. Detection and Prevention. Firm shall maintain controls designed to prevent and detect unauthorized access, intrusions, computer viruses and other malware on its information systems in compliance with industry standards to protect against a Security Incident. Firm networks used to access or store Liberty/Customer Information must have security controls that are designed to detect and prevent attacks by making use of network layer firewalls, modern anti-malware, and intrusion detection/prevention systems.

2.7.2. Monitoring and Logging. Firm shall implement and maintain monitoring controls designed to (i) detect and alert on both known threats and unusual activity (ii) ensure log integrity to prevent against tampering, (iii), be reviewed regularly to identify anomalies, (iv) retain event and activity logs for a minimum of three (3) years.

2.8. Physical Security

2.8.1. Security of Facility. Firm shall store all Liberty/Customer Information securely with appropriate physical access controls. Firm shall restrict physical access to data centers and other facilities storing Liberty/Customer Information to authorized personnel only.

2.9. Third-Party Service Provider Management

2.9.1. Third-Party Service Provider Agreements. Firm is required to evaluate the security controls of all its third-party vendors and sub-contractors who will access or receive Liberty/Customer Information and shall obtain such third-party vendors and sub-contractor's written agreement to maintain security controls no less onerous as those required under the Guidelines and this Security Addendum.

2.9.2. Third-Party Service Provider Due Diligence. In particular, such third-party vendors and sub-contractors must use multifactor authentication (MFA) when accessing Liberty/Customer

Information over non-Liberty controlled networks as well as encryption in-transit and at-rest. Firm shall remain liable for its third-party vendor's acts and sub-contractor's acts, omissions or failures to adhere to security controls required under this Security Addendum.

2.10. Vulnerability and Patch Management

2.10.1. Vulnerability Management. Firm shall ensure vulnerability management policies, standards, and procedures based on industry standards have been established, are maintained, and are enforced appropriately.

2.10.2. Patch Management. Firm shall implement and maintain a patch management procedure that deploys security patches for systems used to access or process Liberty/Customer Information. Firm shall apply within forty-five (45) days any critical patches or security updates that have been successfully tested or, in the absence of a successfully tested patch, implement an appropriate control to similarly mitigate risk for where Liberty/Customer Information resides.

3. NOTICE OF SECURITY INCIDENT

In the event of a security incident that affects Liberty/Customer Information, the firm shall notify Outside Counsel Partnerships immediately, and in any event within seventy-two (72) hours of detection. Notification of a security incident shall be made to Liberty using the following email address:

3PSIncidentResponse@libertymutual.com

Security incident notifications shall include at a minimum and where possible (i) root cause analysis, (ii) source and destination IP addresses, (iii) event logs (network, system, web) indicating unique identifiers (iv) remediation plan, and (v) other materials required to comply with applicable law, regulation, industry standards, or as otherwise reasonably required by Liberty.

Firm shall promptly, at no cost to Liberty (i) investigate the security incident and continuously provide Liberty with detailed information about the security incident (including, where possible, the data records concerned, as well as the consequences of the security incident) and a contact point where more information concerning the security incident can be obtained, (ii) take all reasonable steps to mitigate the effects and to minimize any damage resulting from the security incident, and (iii) cooperate with Liberty to provide information in connection with any notice to be sent out to a third party in connection with such security incident, including as required under applicable laws.

4. RIGHT TO ASSESS SECURITY CONTROLS

Liberty reserves the right upon reasonable prior notice, to conduct a limited security risk assessment of the firm's compliance with the requirements of this Security Addendum.

Liberty may conduct (i) an initial risk assessment prior to receiving services, (ii) additional periodic risk assessments, no more than at least annually thereafter, and (iii) risk assessments upon material changes to services, or if a security incident has occurred, and (iv) continuous monitoring and analysis of publicly available security profile information (collectively, "Risk Assessments"), in order to identify the risks associated with the services to be provided.

Firm will promptly complete the due diligence questionnaires in use by Liberty as part of the risk assessment process and to avoid any delay in services and contract execution. Firm personnel must cooperate with Liberty in such risk assessments, which will be conducted using standards such as ISO

27001 or other relevant items as the basis for its evaluation. The risk assessments will be conducted by Liberty or its designated agents at such times as Liberty deems reasonably appropriate. Should any risk assessment reveal what Liberty determines to be material security risks, Liberty will promptly notify the firm of such risks, and the firm will (a) respond to Liberty with a plan to promptly eliminate the risk, and (b) immediately thereafter, eliminate the noted risks.

This Security Addendum is subject to revisions by Liberty from time to time as security requirements change, either by law or industry standard, or at Liberty's discretion.