MORLEY

EXHIBIT-
THIRD PARTY SECURITY & PRIVACY REQUIREMENTS

This describes the information security and privacy process and control requirements of Morley that must be implemented, maintained by Vendor at its own cost and expense, from the effective date of the applicable agreement (the "Agreement") throughout its term. All capitalized terms used but not otherwise defined in this Addendum will have the meanings set forth in the Agreement.

1 DEFINITIONS.

"Affiliate" means an entity that a party controls or is controlled by, or with which a party is under common control. For purposes of this definition, "control" means ownership or more than 50% of the voting stock or equivalent ownership interest in an entity.

"Authorized Persons" means: (i) Vendor's employees who have a need to know or otherwise access Confidential Information (as defined in the Agreement) to enable Vendor to perform its obligations under the Agreement; and (ii) Vendor's vendors, agents, outsourcers and auditors, in each case where permitted under the Agreement, who have a need to know or otherwise access Confidential Information to enable Vendor to perform its obligations under the Agreement, and who are bound in writing by confidentiality obligations sufficient to protect Confidential Information in accordance with the terms and conditions of this Addendum and the Agreement.

"Morley" means the Morley entity that is a party to the Agreement.

"Morley Information" means Morley Confidential Information and Personal Information.

"Personal Information" means information provided to or collected by Vendor by or at the direction of Morley, or to which access was provided to Vendor by or at the direction of Morley, in the course of Vendor's performance under the Agreement that: (i) relates to, describes, identifies, is capable of being associated with or can be used to identify an individual or household (including, without limitation, names, signatures, addresses, telephone numbers, email 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). Personal Information constitutes Confidential Information of Morley as defined in the Agreement.

"Privacy Law" means: (i) all applicable international, federal, state, provincial and local laws, rules, regulations, directives and governmental requirements currently in effect and as they become effective relating in any way to the privacy, confidentiality or security (Personal Infor 1798.81.5 and 201 Mass. Code Reg. 17.00); laws requiring the secure disposal of records containing certain Licensee Data (such as, but not limited to, N.Y. Gen. Bus. Law § 399-H), and all similar international, federal, provincial, state and local requirements; (ii) all applicable industry standards concerning privacy, data protection, confidentiality or information security.

"Process" means any operation or set of operations performed upon Personal Information, whether by automatic or manual means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

"Security Breach" means: (i) any act or omission that compromises either security, confidentiality or integrity of Confidential Information or the physical, technical, administrative or organizational safeguards put in place by Vendor (or any Authorized Persons) that relate to the protection of the security, confidentiality or integrity of Confidential Information on all systems under Vendor's control and/or responsibility, including those of their own third parties; or (ii) receipt of a complaint in relation to the privacy practices of Vendor (or any Authorized Persons) or a breach or alleged breach of this Addendum relating to such privacy practices.

"Services" means the services, deliverables and other obligations of Vendor under the Agreement.

"Vendor" means the person or entity providing services to or otherwise contracting with a Morley entity pursuant to the Agreement.

2 INFORMATION SECURITY PROGRAM MANAGEMENT.

2.1 Vendor shall implement and maintain administrative, physical and technical safeguards to protect the confidentiality, security and integrity of Morley Information that are no less rigorous than requirements of applicable law and accepted industry practices, specifically the International Organization for Standardization's standards: ISO/IEC 27001:2013 – Information Security Management Systems – Requirements.

2.2 Vendor agrees that it shall maintain a disciplinary process to address any unauthorized access, use or disclosure, modification, and/or deletion information by any of Vendor's officers, partners, principals, employees, agents or vendors. Upon Morley's written request, Vendor shall promptly identify for Morley in writing all Authorized Persons as of the date of such request.

3 SECURITY BREACH PROCEDURES. Vendor shall:

3.1 Notify Morley within 24 hours of a Security Breach occurring and provide Morley with the contact information for the employee(s) or group who shall serve as Morley's primary security contact and shall be available to assist Morley 24 hours per day, seven days per week as a contact in resolving obligations associated with the Security Breach.

3.2 Immediately following Vendor's notification to Morley of a Security Breach, the parties shall coordinate with each other to investigate the Security Breach. Vendor agrees to cooperate with Morley, at Vendor's sole cost and expense, in Morley's handling of the matter, including, without limitation: assisting with any investigation; providing Morley with physical access to the facilities and operations affected; facilitating interviews with Authorized Persons and others involved in the matter; and making available all relevant records, logs, files, data reporting and other materials required to comply with applicable law, regulation, industry standards or as otherwise required by Morley.

3.3 Remedy any Security Breach and prevent any further Security Breach at Vendor's expense. Vendor shall reimburse Morley for actual costs incurred by Morley (including without limitation all costs identified in Section 4 below) in responding to, and mitigating damages caused by, any Security Breach, including all costs of notice and/or remediation pursuant to Section 3. Vendor will perform a root cause analysis and provide to Morley a post mortem report, within 10 business days of a confirmed incident, to include:

3.3.a The nature of the Security Breach;

3.3.b Morley Information involved in the Security Breach;

3.3.c Steps Vendor has taken or will take to mitigate any effect of the Security Breach;

3.3.d Corrective actions Vendor has taken or will take to prevent similar Security Breaches from occurring in the future;

3.3.e To the full extent permitted under Privacy Law, Vendor agrees that it shall not inform any third party of any Security Breach without first obtaining Morley's prior written consent, other than to inform a complainant that the matter has been forwarded to Morley's legal counsel.

3.4 Vendor agrees to cooperate with Morley in any litigation or other formal action deemed necessary by Morley to protect its rights relating to the use, disclosure, protection and maintenance of Confidential Information.

4 SECURITY BREACH EXPENSES.

4.1 Vendor will promptly on demand reimburse Morley for any:

4.1.a Expenses incurred to provide warning or notice to Morley's former and current employees, suppliers, customers and other Persons whose Personal Information may have been disclosed or compromised as a result of the Security Breach (the "Affected Persons") and to law-enforcement agencies, regulatory bodies or other third parties as required to comply with law, including Data Privacy Laws, or as otherwise directed by Morley;

4.1.b Expenses incurred either by Morley or through Morley's retention of an independent third-party forensic investigator, legal counsel, or any other third party, to investigate, assess, or remediate the Security Breach and to comply with applicable laws and/or relevant industry standards;

4.1.c Expenses related to the reasonably anticipated and commercially recognized consumer data breach mitigation efforts, including, but not limited to costs associated with the offering of credit monitoring for a period of at least 12 months or such longer time as is required by applicable laws or recommended by one or more of Morley's regulators or any other similar protective measures designed to mitigate any damages to the Affected Persons;

4.1.d Expenses incurred to retain a call center or to develop any internal or external communication materials in order to respond to inquiries regarding the Security Breach for a period of at least 180 days or such longer time as is required by law;

4.1.e Fines, penalties, or interest that Morley pays to any governmental or regulatory authority;

4.1.f Legal expenses incurred in connection with any Security Breach or to address any claims by third parties as a result of the Security Breach or investigation by law-enforcement agencies or regulatory bodies; and

4.1.g Expenses incurred to the retention of a public relations or crisis management firm in order to manage communications on behalf of Morley related to any Security Breach. Without limiting, precluding or reducing Morley's entitlement to damages of any type under the Agreement or Vendor's indemnification obligations or liability to Morley, the expenses stated in the foregoing (a)-(g) are considered additional direct damages of Morley.

4.2 The Vendor agrees to carry Cyber Insurance, in an amount not less than $3 million covering Vendor and Representatives for claims and losses with respect to network risks (such as data breaches, unauthorized access/use, ID theft, invasion of privacy, damage/loss/theft of data, degradation, downtime, failures in electronic and physical security, and breaches of confidentiality).

MORLEY

5 REPORTING AND AUDIT RIGHTS.

5.1 Vendor will at all times maintain one or more of the following (or any applicable successor certifications or audit reports accepted by Morley):

5.1.a An ISO/IEC ISO 27001/27018:2013 certification (the "ISO Certification");

5.1.b A Service Organization Control ("SOC") 1 Type II report (the "SOC 1"); and

5.1.c A SOC 2 Type II report (the "SOC 2") of Vendor's data center(s) and third-party IaaS providers;

5.1.d Data center's Uptime Institute Tier Certification.

5.2 SOC reports shall be prepared in accordance with the AICPA reporting standard, where applicable. Each of the SOC reports shall fully cover the security, availability, integrity, confidentiality, and privacy-related controls of the information systems (including procedures, people, software, data, and infrastructure) that are used by Vendor and its Affiliates and subcontractors in processing Morley Confidential Information. Vendor will, and will cause Affiliates of Vendor and subcontractors to promptly provide a copy of the SOC Reports and/or ISO Certification to Morley upon execution of the Agreement, in no event later than 30 days of receipt, or annually from an unqualified independent auditor for each annual period in which Vendor, Affiliate of Vendor, or subcontractor receives the same. Vendor will promptly notify Morley of any deficiencies identified in any reports. Vendor will promptly address and resolve any such deficiencies to the extent necessary to comply with Vendor's obligations under the Agreement and this Addendum, and notify Morley when any such deficiency is remediated to an acceptable level by Morley. If any deficiency is not promptly resolved, it will be deemed a material breach of the Agreement by Vendor.

5.3 If, in the course of its engagement by Morley, Vendor has access to or will collect, access, use, store, process, dispose of or disclose credit, debit or other payment cardholder information, Vendor 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 Vendor's sole cost and expense. Vendor shall provide to Morley a PCI DSS compliance report and immediately in the event of any of the following (individually, a "Non-Compliance Event"):

5.3.a Vendor learns or has reason to believe that it is no longer in compliance with PCI DSS Requirements and/or PA DSS Requirements; or

5.3.b Vendor undergoes an adverse change in its certification or compliance status with respect to PCI DSS Requirements and/or PA DSS Requirements. Upon the occurrence of a Non-Compliance Event, Vendor will immediately provide Morley with a detailed plan to remediate such Non-Compliance Event not to exceed 30 days of a Non-Compliance Event. In the event Vendor cannot provide, after reasonable prior notice from Morley, validation of its compliance with PCI DSS Requirements and/or PA DSS Requirements and the necessary Compliance Documentation as required under this Agreement, Morley shall have the right to engage a Qualified Security Assessor (QSA) to conduct an audit of Vendor to determine Vendor's compliance with PCI DSS Requirements and PA DSS Requirements, and Vendor shall pay all costs of such an audit. Any such audit shall be conducted by a QSA on behalf of Morley and shall be conducted so as to reasonably

minimize any disruption to Vendor's operations. Vendor shall reasonably cooperate with such QSA, including providing reasonable access to its facilities and applicable personnel necessary to audit and test compliance. Vendor shall implement all remediation measures, and provide a detailed plan as recommended by such QSA as soon as reasonably possible in order either to remain certified as compliant with PCI DSS Requirements and PA DSS Requirements or to re-obtain certification under PCI DSS Requirements or PA DSS Requirements. Vendor acknowledges that it is solely responsible at all times for the security of any Payment Information or cardholder data in transit, at rest or in its possession. A failure of Vendor to maintain certification of its compliance with PCI DSS Requirements and/or PA DSS Requirements shall be considered a material breach of the Agreement by Vendor.

5.3.c Vendor agrees that Morley may designate an internal or third-party information security representative to perform on-site security control validations and policy/procedure reviews to include related data centers to determine whether Vendor's security measures for safeguarding information conforms to this Agreement. Vendor will implement system and process improvements identified by the security review process within 30 days of any provided remediation plans.

6 SECURITY STANDARDS.

6.1 Vendor will engage, at its own costs, an independent third party to conduct penetration testing on a yearly basis, including human manual testing, to evaluate the security controls of the Vendor systems, platforms and network layers used to provide the Services; and vulnerability scanning to evaluate Vendor-provided software code, applications, and internet facing servers within the DMZ while following industry standard methodologies. Vendor shall provide Morley with copies of its reports at the time they are available and in no event later than 30 days after receipt for each annual period. Vendor will promptly notify Morley of any deficiencies identified as well as corrective actions necessary for all vulnerabilities to be remediated. Should any critical weakness be identified, Vendor will, and will cause its Affiliates and subcontractors (as applicable) to, undertake corrective actions within seven calendar days of receipt of the report. Should any high weakness be identified, corrective actions shall be undertaken by Vendor, its Affiliates, or subcontractors (as applicable) within 30 calendar days of receipt of the report. Morley will not be liable for any failure, negative impact, system degradation, product failure or system failure related to Vendor's systems due to noncompliance under this Section 6.

6.2 Vendor must review its employees' and vendors' access privileges to Morley systems at regular intervals using a formal process and retain supporting evidence of the review process (approval matrix). Furthermore, access rights of Vendor's employees and vendors to Morley systems or Morley Information must be immediately revoked upon termination of the individual's employment, contract or agreement, or otherwise immediately adjusted upon change in responsibilities in which such access is no longer necessary.

6.3 Systems storing and/or processing Morley Information must reside on an isolated network segment or zone that is firewalled off and is only permitted to connect to Morley instance.

6.4 For PaaS and IaaS instances: Administrative access, including ability to configure and troubleshoot network components and system ports, to systems storing and/or processing Morley Information is prohibited unless it formally authorized, monitored and periodically reviewed by Morley.

6.5 Remote access for administrative purposes into Morley instance is prohibited unless it uses two-factor authentication.

6.6 Vendor will maintain Access Control Lists (ACLs) for networks to ensure that computer connections and data flows are routed to appropriate computers and database resources.

6.7 Morley Information must be encrypted in transit (secure tunneling protocols, i.e., TLS 1.2) and at rest with table or file level encryption of at least 256 AES.

6.8 Systems and applications storing and/or processing Morley Information must be protected by Anti-Virus and Next Generation Endpoint Security software capable of detecting unauthorized activity, such as changes in connections and processes. These software solutions must be automatically updated on a daily basis.

6.9 Vendor must implement security tools (e.g., Intrusion Detection/Prevention Sensors [IDS/IPS], Data Loss Prevention [DLP] and Network Packet Capture) and have authorized representatives on duty 24/7/365 capable of monitoring for suspicious network activity, including the ability to detect leakage of Morley Information within active internal network connections as well as outside the outer firewall and inside the DMZ and network.

6.10 Security tools (e.g., Intrusion Detection/Prevention Sensors [IDS/IPS], Data Loss Prevention [DLP] and Network Packet Capture) should be capable of the following:

6.10.a Maintaining active logs for a period of 128 days online;

6.10.b Retaining archives of logs for a period of one year;

6.10.c Updating within 24 hours of release of a new version or signature/definition;

6.10.d Being restricted from being addressable as in-band network device.

6.11 Vendor’s security tools must include event logs that track the following event information:

6.11.a Alerts

6.11.b Date

6.11.c Time stamp

6.11.d Description

6.11.e Priority level

6.11.f User ID

6.11.g MD5 hash

6.12 Vendor will institute and maintain a “separation of duties” and “need to know” between application development, quality assurance, testing and production environments, along with logical and physical separation between systems, databases and application administration containing Morley Information.

6.13 The implementation of system changes shall be controlled through the use of formal change control procedures and supporting authorization and testing of applications, databases and systems.

6.14 Vendor will implement secure configuration that can detect unauthorized changes to applications, databases, and systems.

6.15 Access to application source code shall be restricted. Vendor will keep and maintain an updated version of all source code for software related to the Services.

6.16 Vendor will regularly update systems that store and/or process Morley Information with the most recent versions, builds, and security-related patches released by the system or application manufacturers. Vendor must implement security-related patches using an automated patch management solution that allows Vendor to log details about patch rollout throughout Vendor's infrastructure.

6.17 Vendor will begin testing new versions of software/hardware supporting the security infrastructure within two weeks of release by the manufacturer, including open-source code vendors, and will complete the testing as quickly as commercially possible unless significant issues are discovered. If significant issues are discovered, Vendor will actively work with the manufacturer or open-source code vendor to resolve those issues and will keep Morley apprised of the situation at least once per week.

6.18 To protect the security, confidentiality and integrity of Morley Information, applications must be configured with the following controls:

6.18.a Data input to applications must be validated to ensure that data entered is correct and consistent with the expected data types.

6.18.b Validation checks and post-check shall be incorporated into applications to detect any corruption and ensure that the processing of stored information is correct and appropriate to the circumstances.

6.18.c Requirements for ensuring authenticity and protecting message integrity in applications shall be identified, and appropriate controls identified and implemented.

6.18.d Audit logs recording user activities, exceptions and information security events shall be produced and kept for a minimum of 90 days.

7 PRIVACY AND PERSONAL INFORMATION.

7.1 **Privacy Program.** Vendor represents and warrants that it has and will maintain a comprehensive information privacy program reasonably designed to address privacy risks relating to the Personal Information and to protect the privacy of the Personal Information; that all Personal Information under the control of Vendor is covered by such program, and that this program includes and will include appropriate privacy processes and controls, including but not limited to:

7.1.a The designation of an employee or employees to coordinate and maintain responsibility for the program;

7.1.b The identification of reasonably foreseeable internal and external material privacy risks, including threats that could result in unauthorized disclosure, access, use, alteration or destruction of Personal Information and an assessment of the sufficiency of any safeguards in place to control such risks. This assessment should account for privacy risks in each area of Vendor's operation, including, but not limited to employee training and management, and product design, development and research;

7.1.c The design and implementation of reasonable privacy processes and controls to address the risks identified through the assessment described in Section 7(1)(b) and regular testing or monitoring of the effectiveness of Vendor's privacy processes and controls; and

7.1.d The evaluation and adjustment of Vendor's privacy program in light of any circumstances that Vendor knows or has reason to know may have a material impact on the effectiveness of its privacy program.

7.2 **Processing of Personal Information.** Vendor will not collect, retain, use, disclose or otherwise Process Personal Information except: (i) as necessary for the specific purpose of performing the Services, (ii) in accordance with this Addendum and the Agreement, and (iii) as part of the direct business relationship between Vendor and Morley. Without limiting any other obligation of this Addendum, Vendor will collect only such Personal Information (if any) during the course of performing Services as is necessary for Vendor to perform the Services. Vendor will not use Personal Information for its own purposes, or for any other commercial purpose other than the provision of the Services. Without limitation, Vendor will not sell, rent, release, disclose, disseminate, make available, transfer or otherwise communicate (orally, in writing, or by electronic or other means) Personal Information for monetary or other valuable consideration. **By execution of this Addendum, Vendor hereby certifies that it understands the requirements of this Section and will comply with the same.**

7.3 **Cooperation to Facilitate Data Subject Requests.**

7.3.a Vendor will promptly notify Morley in writing, and in any case within two days of receipt, if Vendor receives: (i) any requests from an individual with respect to Personal Information including, but not limited to, opt-out requests or requests for access, correction, deletion or to receive a portable copy of Personal Information; (ii) any complaint, notice, objection or other communication relating to Personal Information or either Party's compliance with applicable law in relation to Personal Information including, but not limited to, allegations that the Processing infringes an individual's rights under applicable law; or (iii) any communication that an individual seeks to fulfill any other right available to such individual under applicable Privacy Law with respect to Personal Information. Vendor will not directly respond to any such request, complaint, notice, or other communication unless expressly authorized to do so by Morley in writing or required by applicable law, and it will provide Morley with reasonable cooperation and assistance in relation to any such request, complaint, notice or communication at no additional charge.

7.3.b Additionally, Vendor shall ensure that it has implemented technical and organizational measures to assist Morley in fulfilling Morley's obligations to respond to any such requests from individuals with respect to Personal Information.

7.3.c Except with Morley's prior written authorization, Vendor will not provide privacy notices, terms and conditions, or similar materials or communications to any individuals with respect to whom Vendor Processes Personal Information in connection with Vendor's provision of Services.

7.4 **Retention and Deletion.** Vendor may retain Personal Information only for the period of time required for Vendor to perform the Services, or such longer period required by applicable law, required pursuant to the Agreement or requested in writing by Morley. Vendor will permanently delete all copies of Personal Information in its possession or control at the expiration of such time period in accordance with any standards provided for deletion of data in the Agreement or, if the Agreement does not provide such

standards, then in accordance with applicable industry standards for secure deletion of Personal Information.

8 ELECTRONIC DISCOVERY.

8.1 Vendor shall maintain end-to-end electronic discovery capabilities consistent with generally acceptable standards and compliant with all regulations and laws. At a minimum, Vendor shall perform the following functions:

8.1.a Upon receiving written notice from Morley to preserve and collect electronic data relevant to a matter, Vendor shall take reasonable and immediate steps to preserve and collect all electronic data relevant to a case;

8.1.b Vendor shall maintain detailed documentation of all activities related to the preservation and collection of electronic data; and

8.1.c At the request of Morley's legal counsel or its designated representative, Vendor shall search collected data and provide the results to Morley or its designated third party.

9 SUBCONTRACTING.

9.1 Vendor will ensure that it continually maintains written contracts with any subcontractors that Process Personal Information and that such contracts obligate subcontractors to comply with all security-, privacy- and confidentiality-related obligations applicable to Vendor and relating to the Processing of Personal Information under the Agreement and this Addendum. Vendor will ensure that any subcontractors comply with the obligations contained within this Addendum applicable to Vendor as if such obligations were directly applicable to such subcontractor.

10 ACCEPTABLE TRANSMISSION & COMMUNICATION METHODS.

10.1 Per the Classification and Protection of Non-Disclosed Information policy, any electronic communication that is classified Confidential Information or Secret Information has to be transmitted by Vendor in an encrypted format as set forth in the methods below. Morley currently offers several options for performing encryption with additional tools coming in the future.

11 SFTP / PGP.

11.1 In the event that internal, confidential or secret information is communicated, the files must be encrypted using PGP encryption. Morley IT Application Support is responsible for the maintenance and implementation of SFTP file transfers.

11.2 Morley has the ability to update the acceptable communication methods with written notification to the Vendor. Vendor will have a reasonable and agreeable amount of time to comply with any revisions to these standards.