SPConnect
A Service Professionals Company

SPCONNECT PRIVACY POLICY

1. CONFIDENTIAL INFORMATION.

(a) Definition of Confidential Information. "**Confidential Information**" is defined as all nonpublic or propriety information, regardless of form, owned or controlled by one Party ("**Discloser**") and disclosed, by or on behalf of the Discloser, to the other Party or any of said Party's employees or agents, including but not limited to attorneys, accountants, bankers, and brokers (individually or collectively, "**Disclosee**"), regardless of whether such disclosure occurs before, on, or after the Effective Date; directly or indirectly; in writing, orally, or by drawings or inspection of equipment, software, or other assets; tangible or intangible; real or personal. Confidential Information includes, but is not limited to: (i) the SPConnect Property; (ii) any information, technical data, or know-how, relating to the SPConnect Property or to discoveries, ideas, inventions, concepts, software, equipment, designs, drawings, specifications, techniques, processes, models, data, source code, object code, documentation, diagrams, flow charts, research, and development; (iii) business methods, business plans or opportunities, business strategies, future projects or products, projects or products under consideration, procedures; (iv) information related to finances, costs, prices, vendors, contractors, and employees; and (v) trade secrets. Confidential Information also includes any information described above that either Party obtains from a third party and treats as proprietary or confidential information. Confidential Information includes any notes, analyses, compilations, studies, summaries, and other material, however documented, containing or based, in whole or in part, on any information described above. Any document or other material provided by Discloser that is labeled "Confidential" is Confidential Information, as defined in this Agreement, although such labeling is not required for a document or other material to be considered Confidential Information under this Agreement.

(b) Exclusions from Confidential Information. Information is excluded from the definition of "Confidential Information" if Disclosee demonstrates that the information: (i) is or becomes publicly known or generally available, other than as a result of a breach of this Agreement by Disclosee; (ii) is known to Disclosee at or prior to disclosure by Discloser; or (iii) is disclosed to Disclosee by a third party, and such disclosure is not in violation of any confidentiality obligation owed to Discloser. Additionally, the restrictions on disclosure in this Section 1 shall not apply to the extent the information is disclosed by Disclosee pursuant to a requirement of a governmental agency or by operation of law; provided however, that Disclosee shall first notify Discloser prior to disclosure, if allowed by law, in order to give Discloser a reasonable opportunity to seek an appropriate protective order and/or waive compliance with the terms of this Agreement and shall disclose only that part of the Confidential Information which Disclosee is required to disclose.

(c) Non-Disclosure Obligation. Using utmost care, each Disclosee shall: (i) hold Discloser's Confidential Information in trust; (ii) secure and protect Discloser's Confidential Information in a manner consistent with the manner in which Disclosee maintains its own Confidential Information; (iii) except to exercise Disclosee's rights or to carry out Disclosee's obligations under this Agreement, refrain from directly or indirectly: (A) using, selling, licensing, publishing, or reproducing Discloser's Confidential Information or (B) disclosing Discloser's Confidential Information to any other Party, or allowing any other Party to inspect, copy, or use, Discloser's Confidential Information; and (iv) take, by instruction or agreement with its employees, consultants, or other agents who are permitted access to Discloser's Confidential Information, appropriate action to satisfy its obligations under this Section 13. The

© SPConnect, LLC | Proprietary & Confidential

obligations of this Section 13 apply to all of Discloser's Confidential Information that is in the possession of Disclosee, regardless of how Disclosee obtains possession of said Confidential Information.

(d) Return or Destruction of Confidential Information. Upon the earlier of the termination or expiration of this Agreement or the request of Discloser, each Disclosee shall promptly either: (i) return all of Discloser's Confidential Information that is in Disclosee's possession or over which Disclosee has control and provide Discloser with a certificate, from a duly authorized representative of Disclosee, that Disclosee has returned all of said Confidential Information; or (ii) destroy all of Discloser's Confidential Information that is in Disclosee's possession or over which Disclosee has control and provide Discloser with a certificate, from a duly authorized representative of Disclosee, that Disclosee has destroyed all of said Confidential Information.

(e) Notification Obligation. If Disclosee becomes aware of any unauthorized use or disclosure of Discloser's Confidential Information, then said Disclosee shall promptly and fully notify Discloser of all facts known to Disclosee, concerning such unauthorized use or disclosure. If Disclosee or any of Disclosee's employees or agents are requested or required (by oral questions, interrogatories, requests for information or documents in legal proceedings, subpoena, civil investigative demand, or other similar process) to disclose any of Discloser's Confidential Information, then Disclosee shall not disclose Discloser's Confidential Information until Disclosee has provided Discloser at least twenty-four (24) hours prior written notice of any such request or requirement, so that Discloser can seek a protective order or other appropriate remedy and/or waive compliance with the provisions of this Agreement. Notwithstanding the foregoing, Disclosee shall exercise its best efforts to preserve the confidentiality of Discloser's Confidential Information, including but not limited to cooperating with Discloser to obtain an appropriate protective order or other reliable assurance that confidential treatment will be accorded Discloser's Confidential Information by such tribunal.

2. DATA PRIVACY AND SECURITY.

(a) Safeguards of Customer Data. SPConnect shall take reasonable steps to safeguard any non-public Personal Data concerning Customer's employees and customers with which SPConnect comes into contact in the course of performing the Services (the "**Customer Data**"). "**Personal data**" is personally identifiable information and data about an individual (e.g. credit card number, social security number) that is protected by applicable data privacy laws. Without limiting the generality of the foregoing, SPConnect shall refrain from selling Customer Data for any reason and shall take commercially reasonable steps to ensure the privacy and security of Customer Data and to protect it against anticipated threats and hazards, including but not limited to unauthorized access to, or use of, Customer Data. If any court or regulatory agency seeks to compel disclosure of Customer Data, then SPConnect shall, if legally permissible, promptly notify Customer of the disclosure requirement and cooperate so that Customer may, at its expense, seek to legally prevent the disclosure of Customer Data.

(b) Unauthorized Intrusions. If a breach of security results in an unauthorized intrusion into the systems of SPConnect that directly and materially affects Customer or their customers, then SPConnect shall: (i) take appropriate measures to stop the intrusion; (ii) report the intrusion to Customer within a reasonable time after discovery of the intrusion; (iii) subsequently report the corrective action taken by SPConnect in response to the intrusion; and (iv) provide reasonable assistance to Customer to support any mandatory disclosures about the intrusion that Customer makes to its affected customers or as required by law. If SPConnect has notified law enforcement agencies about the intrusion, then SPConnect may delay its notification of the intrusion to Customer until authorized to do so by the law enforcement agencies.

© SPConnect, LLC | Proprietary & Confidential

(c) Privacy Regulation. All capitalized terms used in this Section 2(c) that are not otherwise defined in this Agreement have the meanings set forth in the Federal "Privacy of Consumer Financial Information" Regulation (12 CFR Part 40), as amended from time to time (the "**Privacy Regulation**"), issued pursuant to Section 504 of the Gramm-Leach-Bliley Act (15 U.S.C 6801 et seq.). The Parties acknowledge that the Privacy Regulation governs disclosures of nonpublic information about consumers. Each Party shall, with respect to any Nonpublic Personal Information that said Party becomes aware of or receives during the term of this Agreement:

(i) comply with the terms and provisions of the Privacy Regulation, including but not limited to the provisions regarding the sharing of Nonpublic Personal Information;

(ii) refrain from making any changes to said Party's security measures that would increase the risk of an unauthorized access;

(iii) refrain from using any Nonpublic Personal Information, except to the extent permitted by the Privacy Regulation and other applicable federal, State, or local laws; and

(iv) refrain from disclosing any Nonpublic Personal Information about a consumer to any other entity, except as follows:(A) with the prior written consent of the consumer; (B) as necessary to effect, administer, or enforce a transaction that the consumer requests or authorizes; (C) in Connection with servicing or processing a financial product or service that the consumer requests or authorizes, or maintaining or servicing the consumer's account with Customer; (D) with the consent or at the direction of the consumer; (E) to protect the confidentiality or security of Customer's records pertaining to the consumer, service, product or transaction; (F) to protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability; (G) for required institutional risk control; (H) for resolving disputes or inquiries involving the consumer; (I) to provide information to persons holding a legal or beneficial interest relating to the consumer, or acting in a fiduciary or representative capacity on behalf of the consumer; (J) to provide information to insurance rate advisory organizations, guaranty funds, or agencies, or to Customer's attorneys, accountants, or auditors; (K) to the extent specifically permitted or required under other provisions of law; (L) to provide information to law enforcement agencies, a state insurance authority, self-regulatory organizations, or for an investigation on a matter related to public safety; (M) to provide information to a consumer reporting agency in accordance with the Fair Credit Reporting Act; (N) to comply with federal, State or local laws, rules, and other applicable legal requirements, or a properly authorized civil, criminal or regulatory investigation, or subpoena or summons; or (O) to respond to judicial process or government regulatory authorities having jurisdiction over Customer for examination, compliance, or other purposes as authorized by law.

(d) State Law. Each Party shall comply with all aspects of any applicable State statutes, regulations, or rulings with regard to maintaining the confidentiality of consumer information.

(e) Data Use. Customer agrees that data derived by SPConnect from SPConnect' performance of the Services or input by Customer may be used for the purposes of analysis, including, without limitation, statistical analysis, trend analysis, creation of data models, and creation of statistical rules, except that such analysis shall be performed solely by SPConnect and such analysis shall be performed only in conjunction with data derived by SPConnect from SPConnect' performance of services for other

© SPConnect, LLC | Proprietary & Confidential

customers, input by other SPConnect customers or obtained from third-party data sources. The results of such analysis ("**De-identified Data**") may be used by SPConnect for any lawful purpose. Notwithstanding anything contained in this Agreement, De-identified Data shall not contain (i) any Confidential Information of Customer, (ii) any information that identifies or can be reasonably used to identify an individual person, (iii) any information that identifies or can be reasonably used to identify Customer or its affiliates and their suppliers, or (iv) any information that identifies or can be reasonably used to identify any activities or behaviors of Customer.

© SPConnect, LLC | Proprietary & Confidential