The following is a template designed to assist in drafting a customer letter to critical service providers and suppliers regarding disruptions resulting from, and changes required to cope with, the COVID-19 outbreak. As with all templates, this document provides a basic framework for the broad topics for consideration. Footnotes provide prompts for other general considerations and points for discussion. Each organization has unique risks and considerations that necessarily require customization.

For more information, contact Ronald I. Raether at ron.raether@troutman.com or 949.622.2722 or Sadia Mirza at sadia.mirza@troutman.com or 949.622.2786.

Request for Assurance from Critical Vendors of Operational Preparedness to Address COVID-19 Template

[Date]

[Vendor Name]

Dear [Insert Name]:

[Business Name] (the "Company") has identified [Insert Vendor Name] ("Vendor") as a critical service provider or supplier for our Company's operations. In light of the operational risks posed by the outbreak of the coronavirus ("COVID-19"), we are requesting that Vendor submit a response to the Company describing Vendor's plan of preparedness to manage the risk of disruption to its services and operations (the "Plan").

Responses are to be provided to the Company as soon as possible and in no event later than [Insert Number of Days (e.g., 15, 30, 45)] from the date of this letter. Please submit your responses in writing to [insert email address].

The Plan should be sufficiently flexible to effectively address a range of possible effects that could result from the outbreak of COVID-19. At a minimum, the Plan should include the following:

[Examples Below] [1]

1. Preventative measures tailored to Vendor's specific profile and operations to mitigate the risk of operational disruption, which should include identifying the impact on the Company;
2. A documented strategy addressing the impact of the outbreak in stages (e.g., 30-60-90-120-180 days), so that Vendor's efforts can be appropriately scaled, consistent with the effects of a particular stage of the outbreak, which includes an assessment of how quickly measures could be adopted and how long operations could be sustained under different stages of the outbreak;

[1] The "Plan" requirements listed here are provided as examples of items that should be considered. Additional requirements may be necessary or warranted based on Company's risk assessment or technical or regulatory environments. Consult with counsel on questions related to this issue.

3. Assessment of all facilities (including alternative or back-up sites), systems, policies, and procedures necessary to continue critical operations and services if members of Vendor's work force are unavailable for long periods or are working off-site, including an assessment and testing as to whether large scale off-site working arrangements can be activated and maintained to ensure operational continuity. This would also include an assessment and testing of the capacity of the existing information technology and systems in light of a potential increase in remote usage;
4. Employee protection strategies, critical to sustaining an adequate workforce during the outbreak; and
5. Assessment of the preparedness of critical service providers and suppliers to Vendor's operations.

We would also like to take this time to remind you of the importance of maintaining appropriate controls to safeguard Company's systems and information ("**Company Confidential Information**"). In addition to the security requirements outlined in the agreement between the Company and Vendor, we request you implement the following measures when shifting to a remote workforce, as appropriate to your operations:

[Examples Below] [2]

6. Implement multifactor authentication (MFA) on all VPN connections to increase security. If MFA is not implemented, require remote workers to use strong passwords.
7. Update VPNs, network infrastructure devices, and devices being used to remotely connect into work environments with the latest software patches and security configurations.
8. Raise employee awareness to the increased risk of cyberattacks including, specifically, social engineering attacks.
9. Assess risks of information storage and disposal, which will be most prevalent if paper files are being brought home or if information is being stored locally or on portable devices.

If you have any questions or concerns regarding the above, please do not hesitate to contact [Insert Contact Name] at [Email Address]. We value our relationship with you, and we look forward to getting through this time together.

Sincerely,

Insert Name

---

[2] As with the "Plan" requirements, the measures listed here are examples of items that should be considered. Additional requirements may be required. Consult with counsel on questions related to this issue. Also see Troutman Sanders' publication, *COVID-19 Warrants Modified Cybersecurity for Work-At-Home*, for a discussion relating to what constitutes "reasonable security procedures" in the wake of COVID-19 and NIST Special Publication 800-46 Revision 2, *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security*, for information pertaining to securing remote work environments.