



Date: June 8, 2020

Important Updates on our Financial Stability, Operational Capability, Service Levels and our Plans for Continued Safety

Dear Valued Client,

Trust all is well with you. I last shared with you an update on how we enacted our initial safety response and reached operational stability. I am writing again to thank you for the privilege of being your partner and also to keep you informed on how we are doing. In summary, our Associates are continuing to be productive and are delivering service levels at par with our pre-COVID performance. This is evident from the results of our Associate Surveys, Client Surveys and operational metrics that my fellow Board members and I are regularly monitoring.

You are our most important stakeholder and your interests are our highest priority. Our enduring partnership that you allowed us to establish has fueled our growth and enabled our Associates to thrive professionally. It is incumbent on us to watch out for your interests every day, especially during a crisis, and give you deeper insights into how we are doing.

Accordingly, I am sharing below a 7-8-minute read detailing our financial stability, service levels, workforce productivity, cyber security and return-to-work perspectives.

We continue to be financially strong and resilient. Early on in this crisis, we took a bearish approach for the short term while we maintained our bullish outlook and related investments for the long-term. We also formed a Finance Task Force to prepare for a variety of scenarios and we decided to shore up our reserves for the worst-case scenarios we modeled. We were pleasantly surprised to see how steady demand has remained and how stable our profits have been in the past three months. We believe there are several reasons for this. For one, the industries we serve have not been as severely affected as the rest of the economy. Second, our Clients are leaders in their respective markets and almost all of them are continuing to weather the storm better than others. We are not hearing our Clients discussing a material reduction in their technology budgets. Our “value-for-money” model and “brand-of-trust” that we worked very hard for, are also paying off and we are actually seeing an uptick in business from some of our Clients. Third, we were quick in implementing the recommendations from our Finance Task Force and these measures made us more efficient.

While we are happy that we are growing, counter to our bearish expectations, we understand that it is too early to let our guard down. We believe that as the world overcomes the pandemic, as it surely will, the efficiencies we are gaining and the collaboration capabilities we are building will become economic tailwinds. While we may or may not deliver the spectacular growth of prior years, we know that consumer behavior has been reshaped by this pandemic and we are well positioned to meet the more urgent demand for omnichannel experience, digital service and e-collaborations.

Our performance and service levels continue to stay strong. Our Program Management Office (PMO), known in our early days as the Quality Management Office (QMO), has been operating in parallel to our delivery teams for years to independently audit the quality of our services and deliverables. The PMO’s mission has been expanding in recent years to become custodians of our “Brand of Trust”. As such, they review projects to ensure that we are keeping our promises, adhering to timelines and delivering high quality services. In the last ten

weeks, they have become critical for us in understanding how we are performing in the work-from-home mode, with metrics and results from customer surveys, vis-à-vis our normal performance levels. In summary, I am happy to report that our performance and service levels are at par with our pre-COVID level metrics. You may find a few of the metrics informative and therefore I am providing them here (pre and post COVID numbers): Schedule adherence 97-97, Velocity adherence 97-96, SLA adherence 99-100, Productive work hours 98-99, Cost adherence 98-98, Quality adherence 99-98.

Our workforce is engaged and productive. Our Chief People Officer and our Chief Operating Officer are closely monitoring how engaged our Associates are with their work, with colleagues and with customer partners, and whether our productive work hours curve is staying stable or not. To gauge these, they had discussions with team leaders, conducted Associate surveys and monitored work. The results they presented are showing a uniform increase in the actual number of hours Associates are working. While some of this gain may be due to increased amount of time spent in meetings, it is still significant. We are happy with this boost in productivity but concerned about burn out. Hence, our HR has taken up two key initiatives – one, train team leaders to reduce frequency and length of meetings; two, help Associates plan their day better. We have seen a reduction in hours spent on meetings, but the number of work hours remains high. Our HR Leaders will work towards bringing this down to an acceptable level. Increase in work hours, combined with robust performance levels, are also indicative of the fact that our Associates are rising up to the occasion and performing well for you, continuing to remain invested in your satisfaction and attending to the minutest of details with their skill and craft.

Our cyber security efforts, while continuing to be improved, are fully operational and working. As your teams may already be aware, our delivery centers located in India are SSAE 18 SoC2 Type2, ISO27001 and HITECH compliant and are annually audited and certified. In the early days of the pandemic, our Enterprise Risk Management Group (led by one of our Board members) alerted us to the possibility that the risk of cyber threats will increase substantially with our Associates working from home on their Wi-Fi networks and no longer sitting behind corporate firewalls. As part of our routine assessments and improvements process, in 2019 we had contracted with Ernst & Young LLP to (1) perform an “Information Security Review”, and (2) identify, assess and prioritize our enterprise-wide risks. While these SOWs are still in progress, this ongoing work, our annual certification process, and the related measures we implemented enabled us to be better prepared for this remote-work environment. Some of the measures we implemented include:

Devices: We made a decision early on that all our Associates will use laptops or desktops that we or our Clients provided and not personal devices. In the initial work-from-home phase, we had about 1% of our India workforce and 18% of US workforce using personal devices for work. In these cases, we allowed access after we (or our Clients) either hardened the device or provided them with a virtual desktop environment. We have now replaced all the personal devices for our India Associates with our hardened corporate devices. We are in the process of replacing our US Associates’ devices with hardened corporate or client provided devices and will accomplish this by end of July. Our hardened devices have end-point security, port blocking, encrypted hard drives, multi-factor-authentication for productivity apps, content and URL filtering, intrusion prevention and end point firewalls. Operating systems and security software of these devices are kept up to date by our ICT team.

Connectivity: Our Associates are using VPN connections to connect to our Clients’ networks, either directly or through our network and then through a VPN tunnel to our Clients’ network. The VPN

connections that our Associates are using are all leveraging multi-factor-authentication to provide even more security and counter certain behavioral risks.

Training: As one researcher found, 99% of cyber threats need human interaction to succeed. Unfortunately, with COVID19, phishing emails have exploded in volume. We understand that a trained team is a safe team. We have been regularly updating our Associates on best practices and security tips. We have NDAs, periodic orientations and training on Cyber Security for all of our Associates. Our ERM team is now planning for a more thorough approach to train our Associates be fully conscious of how much is at stake, ensure that they are fully compliant with all security policies and transform them from a point of vulnerability to being the first line of defense against cyber threats.

Continuous improvements to Cyber security. We understand that Cyber security is a continuous endeavor. We are further enhancing our security by implementing a range of controls across our corporate network and end points, including end-point platforms (to protect against malware, ransomware, peripheral controls, endpoint DLP, detection and response), CASB solution (to provide controlled access to O365 from restricted devices to prevent access from non-approved end point devices) and also work with our Client IT teams to similarly control and limit our US Associates' access to Client networks, from authorized devices. These initiatives will be rolled this month

Return of our Associates to our offices and our Clients' offices. Adhering to the guidance of our COVID19 Task Force Coordinators, we have informed our Associates that they will continue working remotely at-least until October 1, 2020, and later if needed. We have also kept key contacts of our Clients' informed about this. Almost all of our Clients are supportive of this decision and we are in continued discussions with the remaining Clients. Our Board and most of our Clients believe this is a prudent decision as this gives us time to think through all the concerns that need to be addressed and develop a risk management plan. We are currently in the process of shortlisting an advisory firm who can help us identify a comprehensive list of items to be considered. We are also proposing to work closely with our Clients' Task Force Leaders, key contacts and vendor management teams to develop risk management plans that are suitable for each Client while ensuring the safety of our joint teams.

Thank you for your time, and if you need further information on any of these, please do not hesitate to reach out to me.

Sincerely,

Kalyan Kodali ("KK")
CEO