Steve Freddo
Director, Billing Operations
athenahealth, Inc., on behalf of VVC Holding Corp.
311 Arsenal Street
Watertown, MA 02472
sfreddo@athenahealth.com

Via Email

Alejandra Galvan
Genpact (UK) Limited
Alejandra.galvan@genpact.com

Re: Professional Services Agreement, dated February 7, 2019 (the "Agreement"), between VVC Holding Corp. ("Virence") and Genpact (UK) Limited ("Contractor" and, together with Virence, the "Parties" and each, a "Party")

April 7, 2020

The Parties acknowledge the challenges associated with the COVID-19 pandemic ("**COVID**") and desire to memorialize certain measures that Contractor is taking in response to COVID. In an effort to promote the safety of Contractor's workforce, while minimizing potential business disruption, it is our understanding that Contractor is implementing remote "Work From Home" policies for its employees during the outbreak.

Virence acknowledges and agrees that effective as of the date this letter (the "**Letter**") is countersigned by Contractor and until such time as Contractor determines in its sole but reasonable discretion that it is no longer necessary for its workforce to work remotely as a result of COVID, Contractor employees may perform Contractor's obligations under the Agreement remotely (the "**Remote Access Period**"), so long as Contractor complies with the security requirements identified on Annex A attached hereto (the "**WFH Security Measures**"). In addition, Contractor will implement certain information security awareness and compliance training modules to provide guidelines to remote employees on handling Virence's confidential information while working from home. Contractor will obtain acknowledgements from such remote employees who have access to Virence's confidential information, wherein such employees agree to maintain the confidentiality of such data and to comply with applicable data privacy and security laws.

Contractor will use best efforts to comply with the Agreement during the Remote Access Period. Virence understands and agrees, however, that Contractor may be unable to comply with certain obligations set forth in the Agreement due to unique circumstances that Contractor employees experience while performing services in their homes. Accordingly, Virence agrees that Contractor shall not be penalized under the Agreement if Contractor cannot fully perform any obligation under the Agreement as a direct result of COVID and the need to work remotely during the Remote Access Period. Notwithstanding the foregoing, Virence does not waive any claims, rights or remedies Virence may have with respect to any Contractor contractual obligations not directly impacted by COVID.

Contractor will provide Virence notice when it is scheduled to return to its normal business operations.

In addition to the foregoing, Contractor agrees to comply with the requirements of PCI-DSS throughout the term of the Agreement. Contractor will obtain and provide to Virence a copy of its then-current annual PCI-DSS Compliance Attestation of Compliance (AoC) to Virence upon request, which shall include each payment application used by Contractor in connection with the services.

Except as specifically described in this Letter, the terms of the Agreement shall not be modified or waived.

If the terms set forth above are acceptable to you, please execute this Letter and return the executed copy to Virence. The terms of this Letter will become effective and binding upon your execution hereof.

Sincerely,

Steve Freddo

Steve Freddo (Apr 7, 2020)

Steve Freddo

Director, Billing Operations

cc:

Jessica Collins
General Counsel
athenahealth, Inc.
jecollins@athenahealth.com

Acknowledged and agreed by:

Genpact (UK) Limited

By:_____

Name: Diwakar Singhal

Title: Global Business Leader

Annex A

COVID Security Measures

Contractor agrees to comply with the following security measures with respect to its workforce working remotely during the Remote Access Period. Contractor agrees to work with Virence in good faith in advance of any workflow changes to determine and implement appropriate security measures applicable to any other workforce members impacted by COVID.

1. Each laptop and desktop (each, a "Computer") must have whole disk encryption enabled at all times.
2. Contractor must inventory each Computer over time and monitor the controls implemented. Any exceptions to this agreement found during the monitoring process must be reported to Virence in writing within seventy- two (72) hours and remediated within a timeframe as mutually agreed between the parties.
3. Each Computer must have anti-virus installed in a manner such that the local user cannot disable it.
4. Each Computer must have USB blocking controls installed in a manner such that the local user cannot disable it.
5. Each Computer must have web proxy enforcement configured at the OS level in a manner such that the local user cannot disable it.
6. Each Computer must interact with employees using a regular Windows account (with no admin rights) so that such user cannot install software on the computer.
7. Contractor's VPN must be able to handle all new users to account for each workforce member who supports Virence working from home.
8. Each Computer must have an OS firewall installed and enabled in a manner such that it is always on and the local user cannot disable it.
9. Users are instructed to not save copies of any Virence data to the local PC (screenshots, etc).

Contractor must maintain adequate records, and provide such records to Virence upon request, demonstrating Contractor's compliance with the requirements set forth above, including, without limitation:

1. Proxy configuration - access to websites is controlled via local host agent that enforces proxy usage at all times.

2. USB blocking - enforcement of USB blocking at all times on the local host using an agent

3. Whole disk encryption - enabled on all Computers

4. OS Firewall - enabled and always enforced on all Computers

PCI-Specific Security Measures

While all reasonable endeavors shall be taken to ensure that the requirements of PCI-DSS are complied with during the Remote Access Period, there is a risk of potential card data leakage due to inadequate physical security controls at home, the inability to physically monitor employee activities during this period, and voice calls being taken outside a controlled environment. Except to the extent caused by the gross negligence or willful misconduct of Contractor, Contractor shall not be responsible for a failure to comply with the PCI-DSS requirements to the extent that Contractor relies on, and complies with, the Virence-provided standard operating procedure around card payment processing in respect of such PCI-DSS requirements.

People

One of the best ways to mitigate that risk is to create and maintain a culture of security within the organization. Examples of controls for remote workers include:

- Implement a security-awareness program (PCI DSS Requirement 12.6), delivered at the start of employment and at least annually thereafter, to make sure that all personnel are properly trained and knowledgeable about the business's security policies and procedures. This includes reviewing security policies and procedures with all in-house and at-home/remote agents at least annually to ensure that security processes and procedures are not forgotten or bypassed. As a best practice, consider requiring personnel to acknowledge the security policy as part of their daily sign-in process.
- Particular attention must be given to home workers. Some of the examples of controls may be difficult to implement. Organizations should evaluate the additional risks associated with processing account data in unsecured locations and implement controls accordingly. All staff should be made fully aware of the risks related to remote or home-working and what should be required to maintain the ongoing security of systems, processes, and equipment supporting the processing of telephone-based payment card data.
- Securing systems and data located in home-worker environments can be challenging and difficult to enforce. At a minimum, home workers should be required to ensure that any systems they use to process account data, and any account data to which they have access, is securely maintained and not accessible to any unauthorized individual.

Process

The physical environment within which an office worker or home worker is taking card payments over the telephone should be effectively monitored and access controlled. Examples of required controls include:

- Ensure that at-home/remote workers use a multi-factor authentication process when connecting to the telephone environment or to any systems that process account data.
- Restrict physical access to media containing payment card data, such as call or screen recordings, as well as networking/communications hardware.
- If account data is ever written or printed on paper, ensure it is securely stored, then shredded when no longer needed. If any part of the telephone environment is outsourced to a third-party service provider, both the entity and service provider should clearly understand their responsibilities for securing their respective systems, processes, and personnel, and document accordingly.

Technology

By limiting exposure of payment data in your systems, you simplify scope and validation, reducing the chance of being a target for criminals. Examples of recommendations for remote workers include:

- Require all personnel to use only company-approved hardware devices- e.g., mobile phones, telephone handsets, laptops, desktops, and systems. This is especially relevant to remote/at-home working, ensuring that the entity can maintain control of systems and technology supporting the processing of telephone-based payment card data.
- Ensure that all desktop/terminals, in remote/at-home working environments:
    - Have personal firewalls installed and operational.
    - Have the latest version of the corporate virus-protection software and definition files.

    - Have the latest approved security patches installed.
    - Are configured to prevent users from disabling security controls.
- For the home/remote worker supported as an extension of the entity's network, make sure that their environment (e.g. network and other technology) is secure in accordance with the PCI DSS requirements.