



Capital One Bank (Canada Branch)
161 Bay Street, 19th Floor
Toronto, ON M5J 2S1

April 2, 2020

In response to the Coronavirus (COVID-19) pandemic, Capital One Bank (Canada Branch) ("Capital One") and Concentrix Technologies Services (Canada) Limited ("Supplier"), together known as the "Parties", agree to the following accommodations to the February 28, 2005 Master Services Agreement (MIN-13326) (the "Agreement"), and the January 1, 2019 Third Revised and Restated Statement of Work (CW80384) (the "SOW"):

The "Services Location(s)" specified in the SOW are hereby amended as follows during the Accommodation Period: In addition to providing Services from the Capital One approved Supplier Facilities, Supplier employees, agents or representatives providing Services to the queues listed below shall be allowed to work from home ("Accommodation").

Additionally, this letter authorizes Supplier to transport desktop computers and associated equipment needed for Supplier to provide the Services in accordance with this letter ("Equipment") to Supplier's employees', representatives' and agents' homes.

The Accommodation applies from a future date to be determined by Capital One in a subsequent communication ("Effective Date"), until Capital One determines in its sole discretion that the Accommodation is no longer required ("Accommodation Period"). The Accommodation Period will be reviewed every two (2) weeks until normal operations can be resumed at the approved, corporate location stated in the contract. Capital One reserves the right to shorten the Accommodation Period in its sole discretion upon notice (email acceptable) to Supplier.

This Accommodation applies to the following operations only, and is not an amendment of Services Location(s) for any other Supplier employees, agents, or representatives:

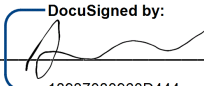
- The following queues, as described under the SOW:
 - English Customer/Fraud Servicing supporting Branded, Hudson's Bay, Saks and Costco (collectively, the "Portfolios")
 - French Customer/Fraud Servicing supporting all Portfolios
 - English & French Customer Servicing supporting all Portfolios

The SOW generally contains Service Levels, Service Level Credits and Performance Incentives (collectively, the "Performance Metrics") applicable to the queues described above. Unless otherwise agreed to by the Parties, such Performance Metrics shall continue to apply. The Parties may meet and discuss the need to potentially adjust or waive respective Performance Metrics as a result of the circumstances.

In the event that any employee, agent or representative will support the Services from outside the approved Supplier Facilities, Supplier will ensure that the attached requirements are

communicated and acknowledged in writing by each such individual. Such written agreements shall be retained by Supplier, and provided to Capital One upon its reasonable request.

Capital One Bank (Canada Branch)

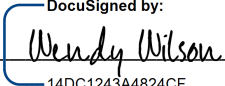
By:  DocuSigned by:
18937080960D444...

Printed Name: Holly Jackson

Title: Vice President, Card Operations

April 2, 2020

**Concentrix Technologies Services
(Canada) Limited**

By:  DocuSigned by:
14DC1243A4824CF...

Printed Name: wendy wilson

Title: Corporate Counsel

April 2, 2020

In addition to the Accommodation of services provided above, Supplier agrees to the deployment of the following controls specific to the management of the Information Technology environment:

- Maintain an active and up to date listing/tracker (to include names, addresses, role, and scope of work) of all Supplier employees, agents, and representatives which have been provided Supplier desktops or Capital One laptops and are allowed to work from home to support Capital One and share such list with Capital One upon request.
- Establish a mechanism to track the removal and return of the assets used to manage services for COF.
- Ensure all equipment is hardened, patched for known vulnerabilities and configured in alignment with Capital One requirements before distribution.
- Ensure distribution of power, network cables, monitors and wifi adapters as necessary for employees, representatives and agents so as not to disrupt the Services.
- Ensure employees, representatives and agents are provided privacy screens and understand the expectation to use the privacy screens to obscure the screen on Equipment provided.
- Ensure connection to dedicated ISP via wifi adapter if applicable.
- Ensure completion of computer based training for all employees to reinforce expectations regarding information security, data handling, confidentiality and other applicable expectations.
- Ensure devices are limited to only the applications that are necessary for the delivery of Services to Capital One.
- Ensure secure mechanisms are established, and sufficient resources are assigned to enable ongoing remote support for the employees, agents and representatives providing services to Capital One.
- Ensure that antivirus/anti-malware software capabilities are deployed on the Equipment.
- Ensure that monitoring of employees, agents and representatives use of Equipment for unusual behaviors that may indicate fraud, take appropriate actions to manage unauthorized exposure, and notify Capital One of such behavior (e.g. abnormal login patterns, etc).
- Ensure that processes are in place to terminate remote accesses and retrieve Equipment from an employee, agent or representative upon their termination, or termination of the Accommodation Period, whichever is earlier.
- Partner with Capital One, to create, define and deploy appropriate solutions to reduce the cyber risk threat landscape, including controls to address:

- Remote-wipe capabilities on the Equipment.
- Off-net browsing restrictions
- Full-disk encryption for the devices

In addition, Supplier acknowledges that its obligations under the Agreement and SOW with respect to Safeguarding of Data, Privacy and Confidentiality, apply equally whether Supplier's employees, representatives and agents work from home or from the approved Supplier Facilities. Beginning as of the date of signature of this document, until the end of the Accommodation Period, Supplier shall provide Capital One with notice as soon as possible upon discovery that (a) Supplier's ability to comply with information security, Safeguarding of Data, Privacy and Confidentiality obligations as outlined in the Agreement and SOW is limited beyond what has already been accepted by Capital One, as set out herein, or (b) additional modifications are necessary to the work from home solution Supplier created and communicated to Capital One. In either case, Supplier will work with Capital One to ensure that adequate alternative controls are in place prior to making any changes to the Accommodation terms and conditions.

Capital One acknowledges that, while the following measures will continue to be required of Supplier's employees, representatives and agents as included in the Acknowledgment, Supplier cannot be held responsible for physically monitoring the following measures in the work from home environment:

- Portable electronic devices, which include but are not limited to mobile devices and other electronic media recording devices are prohibited unless leveraged to directly support multi-factored authentication controls as defined in associate/employee agreement;
- Work space should be maintained as paperless, with no use of paper, pen, pencil or other printed or recording material;
- Equipment and information must be secure from inadvertent and/or unauthorized access or theft at all times (all devices are stored in locked cabinet or drawer when not in use); and
- Dedicated workspace during working hours is separate from, or not accessible by, others; i.e., both Supplier and Capital One documents/computer screens cannot be viewed by others.

I agree that if requested by Capital One, I will provide an artifact evidencing the completion of the above requirements. I hereby attest that equipment has been configured in accordance with the configuration standards conveyed by Capital One and the requirements outlined above.

Supplier Technology Executive or Delegate Signature: _____

Printed Name: _____

Title: _____

Requirements To Be Communicated by Supplier and Acknowledged in Writing by Supplier's Employees, Agent or Representative

As an employee, agent or representative of Concentrix Technologies Services (Canada) Limited who has access to Capital One systems and is working at a location other than my regular corporate location, I acknowledge receipt of, and agree to, the following:

Warning Message for System Access:

Access to Capital One's systems is restricted to authorized users of Capital One Financial Corp and its subsidiaries and branches thereof (COF), and for authorized purposes. Users must have no expectation of privacy with respect to such usage. All software, data, transactions and other electronic communications may be monitored, without notice to the user. Programs, data and information contained herein are the property of COF and must be treated as strictly confidential. Unauthorized use is prohibited, and violators may be subject to disciplinary actions including loss of employment, civil and criminal prosecution.

1. The assigned corporate remote computing device must only be used
 - a. by the employee, agent or representative to whom it is assigned,
 - b. for COF business, and
 - c. at the home address on record with the Supplier of the employee, agent or representative to whom it is assigned, or at the Capital One approved Supplier Facilities.
2. Employees, agents and representatives of Supplier shall connect to the approved corporate VPN prior to accessing the internet and/or transmitting COF information.
3. Employees, agents and representatives of Supplier assigned to a corporate remote computing device, must safeguard all COF information resources against unauthorized, accidental, or intentional access, modification or destruction.
4. Printing COF information and/or copying or storing COF information on removable drives/media is not permissible and capabilities shall be disabled.
5. Employees, agents and representatives of Supplier may not capture any data or images (written notes, pictures, or video) of any COF sensitive information accessed on the corporate remote computing device on any external media (including paper) or device (including phones).
6. Employees, agents and representatives of Supplier may not share any assigned userIDs, passwords or authentication solutions with anyone. This includes but is not limited to: userIDs and/or passwords for network systems, computer accounts, encryption software, client authentication or authorization information.

7. Employees, agents and representatives of Supplier will keep any authentication tokens in a secure location separate from the assigned corporate remote computing device when not in use.
8. Employees, agents and representatives of Supplier may not replace, tamper with or remove anti-virus, malware, or firewall software.
9. Employees, agents and representatives of Supplier must ensure that the assigned corporate remote computing device is kept physically in a locked room, or in a secure environment when not in use. Employees, agents and representatives of Supplier will not leave the assigned corporate remote computing device unattended for any reason, without ensuring the computer is locked.
10. Privacy screens shall be used with the assigned corporate remote computing device at all times to ensure COF data is not visible to others.
11. Only authorized IT personnel should install, reconfigure or otherwise adjust any computer system's hardware or software.
12. Employees, agents and representatives of Supplier may not download, copy, or use any other software, other than those applications installed by authorized IT personnel.
13. Employees, agents and representatives of Supplier may not store any personal data, including but not limited to: music, pictures, or movies locally on the assigned corporate remote computing device.
14. Employees, agents and representatives of Supplier shall ensure that sensitive or confidential conversations, including conversations that might reveal consumer personal information, are not overheard.

You acknowledge by receipt of this agreement and authorization to work from your approved home location that you understand your obligations to maintain the confidentiality of COF information for which you may come into contact. Should you believe confidentiality may have been breached, you will notify your supervisor immediately who will in turn follow protocols to notify Capital One. Failure to comply with the terms of this agreement may result in removal from the engagement and/or disciplinary action as established by your employer.

You acknowledge that all other terms and conditions of your employment agreement with Concentrix remain in effect. In the event of any conflict between the terms of this Acknowledgment and the terms and conditions of your employment agreement with Concentrix, the terms of this Acknowledgment prevail.

Employee/Agent/Representative Last Name _____

Employee/Agent/Representative First Name _____

Employee/Agent/Rep Signature _____

Date _____

Employee/Agent/Representative Address _____

Supplier Approver Signature _____ **Date** _____

Asset Tag Number _____

Service Tag Number _____