Cash Management Services Agreement

SMBC Documentation Portal Schedule

SMBC Bank International plc

This schedule is supplemental to the Cash Management Services Agreement (the "Agreement") between the Bank and the Customer. Expressions defined in the Agreement have the same meanings in this schedule.

1. General Provisions Applicable to the SMBC Documentation Portal Services

(a) Use of SMBC Documentation Portal Services. All of the Services may be accessed through our SMBC Documentation Portal" service available through our web site, https://www.smbcdigital.com. By using these SMBC Documentation Portal Services, you agree to the terms and conditions set forth in this Schedule and the other documents and agreements referred to herein. You understand and acknowledge that the SMBC Documentation Portal Services may be accessed through the use of signatures, identification codes, authentication passcodes, passwords and Digital Token codes and that we are entitled to rely upon any instructions or information provided by anyone using these signatures, identification codes, authentication passcodes, passwords and Digital Token codes and treat such instructions or information as having been authorised and approved by you.

(b) Internet Access and Use. Please be advised that if you elect to use our SMBC Documentation Portal Services through https://www.smbcdigital.com you will use point and click procedures that indicate your instructions to us or your acceptance or agreement to specific terms or provisions. These procedures constitute "electronic signatures" that are binding on you. We will from time to time provide information electronically to you that constitutes "electronic records" under applicable law.

(c) System and Security Requirements Associated with Internet Use. If you elect to use these services through https://www.smbcdigital.com you agree to follow all security measures and advice provided by SMBC through https://www.smbcgroup.com/security/index.html/ and the security procedures and recommendations described below. As the Bank continues to enhance the security controls, we deploy for our Cash Management Services to protect you and the Bank, from time to time it may be necessary for us to change our systems, Digital Tokens or security procedures. It may also be necessary for you to need to update your systems or security procedures. You agree to comply with these changes in order to continue accessing SMBC Documentation Portal Services.

2. SMBC Documentation Portal Service Summary and Sign-Up

(a) SMBC Documentation Portal. SMBC Documentation Portal provides documentation download services - such as account statement, interest statements and other communication from the Bank - through https://www.smbcdigital.com. Full details of all documents available can be found through the Bank's web page https://www.smbcgroup.com/emea/products-services/cash-management/

(b) SMBC Documentation Portal Sign-up Procedures. Please review, sign and return to us the "SMBC Documentation Portal Subscription Form" that will be sent to you by the Bank. The "SMBC Documentation Portal Subscription Form" requires you to:

i) select all the Services you wish to subscribe to through the SMBC Documentation Portal Subscription facility, and

ii) designate the user(s) you would like to be given access to the SMBC Documentation Portal Subscription, and provide his, her or their e-mail address and phone number. Upon completion of the signing of the necessary Agreement(s) and "SMBC Documentation Portal Subscription Form", the Bank's Information Security personnel will contact your designated user(s) to deliver the confidential Authentication Code.

(c) SMBC Documentation Portal Setup Procedures. Full details of the procedures associated with the initial log-in and document download for your authorised user(s) can be found in the "SMBC Documentation Portal User Guide" and/or other instructions that will be provided to you by the Bank.

3. SMBC Documentation Portal Security

(a) Protecting your Account. It is your obligation to establish and implement policies, procedures and a system of controls over the use of the SMBC Documentation Portal, and to perform such internal and external audits as you believe appropriate to assure that the services are only used in an appropriate and proper fashion. In that regard, we strongly recommend that:

i. Identifying Information, Authentication Passcodes, and Digital Tokens are specific to each authorised user and should never be shared.

ii. Identifying Information, Authentication Passcodes, Digital Tokens or any other security devices should never be displayed in an area accessible by others.

iii. Digital Tokens including on mobile devices should never be left unlocked and unattended.

iv. PC's or other devices used to access the SMBC Documentation Portal should never be left unattended whilst a session is active.

v. SMBC Documentation Portal Services should only be accessed from a non-public (personal or corporate owned) PC or device on which virus protection software and the latest Operating System, Browser and Security updates have been installed and continue to be promptly maintained when they become available from the manufacturer.

vi. PCs or other devices used to access the SMBC Documentation Portal should be routinely scanned using your virus protection software to detect and remove any viruses found. Undetected or unrepaired, a virus may corrupt and destroy programs, files and even hardware. You agree that the Bank is not responsible for and shall have no liability for any virus that you may encounter using SMBC Documentation Portal Services.

vii. Users should always exit the system by clicking the Logout button from the menu after using the SMBC Documentation Portal.

viii. You should notify the Bank immediately if you suspect that Identifying Information, Authentication Passcodes, or Digital Tokens may have been compromised and become known to any unauthorised individual. Such Identifying information, Authentication Passcodes or Digital Tokens should be terminated immediately by the BCSA or CSAs.

(b) Monitoring of Authorised User Security Compliance. You are responsible for instructing all authorised users as to each of the procedures for maintaining security of Identifying Information, Authentication Passcodes, Digital Tokens or any other security devices set forth in Clause (a) above. You are also responsible for ensuring all Authorised Representatives continue to maintain adherence to these security procedures.

(c) Your Obligation to Examine Records and Report Discrepancies.

i. We provide various confirmations and statements of your activities. It is your obligation to examine those statements and report any discrepancies.

ii. You agree to examine your statement promptly and to notify us immediately of any discrepancy between the statement and your other account records (other than one relating to an employee's access level, which should be promptly reported to the Bank).

(d) The SMBC Documentation Portal and adherence to Strong Customer Authentication (SCA)

In order to access SMBC Documentation Portal Services you must adhere to our procedures for Secure Customer Authentication (SCA) as defined in the "Strong Customer Authentication Schedule"

4. Your Authorised Users

You agree that all authorised users who have been provided access to the Services through the use of identifying information, Authentication Passcodes, and Digital Tokens (or by any other means whether through the Customer's negligence or not) will be considered acting with your full authority in their use of the SMBC Documentation Portal. We are authorised

and empowered to rely and act upon instructions received providing your identifying information and Authentication Passcodes as part of an online session.

5. Data Protection

Any Processing of Personal Data under the service agreement shall be performed in accordance with the applicable Data Protection Legislation. However, unless explicitly agreed otherwise, the Bank is not responsible for compliance with any laws applicable to the Customer or the Customer's industry that are not generally applicable to the Bank as a service provider.