Cash Management Service Agreement

E-Moneyger® 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 E-Moneyger® Services

(a) Use of E-Moneyger® Services. All of the Services may be accessed through our "E-Moneyger® service available through our web site, https://www.smbcdigital.com. By using these E-Moneyger® 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 E-Moneyger® 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, information or transactions provided by anyone using these signatures, identification codes, authentication passcodes, passwords and Digital Token codes and treat such instructions, information or transactions as having been authorised and approved by you.

(b) Internet Access and Use. Please be advised that if you elect to use our E-Moneyger® 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 advices 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 E-Moneyger® Services.

(d) Fees. Our Fees for E-Moneyger® Services will be as set forth in and payable in accordance with Annex 1 ("Fee Addendum") to this Schedule (together, the "Fees"), or as otherwise agreed in writing between us from time to time. We will provide you with a copy of our most recent Fee Addendum upon request. We will provide you with written notice of any changes to the Fees, which will become effective on and as of the date specified in such notice, and which shall in any case be no earlier than sixty (60) calendar days following the date of such notice.

2. E-Moneyger® Service Summary and Sign-Up

(a) E-Moneyger® Services.

E-Moneyger® provides a range of Cash Management Services including Fund Transfers, Balance and Statement Reporting and Foreign Exchange & Money Market Confirmations through https://www.smbcdigital.com. Full details of all services available can be found through the Bank's web page https://www.smbcgroup.com/emea/products-services/cash-management/

(b) E-Moneyger® Sign-up Procedures.

Please review, sign and return to us the "Company Sign-up Form" that will be sent to you by the Bank**.**

The "Company Sign-up Form" requires you to:

i) select all the Services you wish to subscribe to through the E-Moneyger® on-line banking facility, and

ii) designate a Primary Contact Person as well as a Bank Created System Administrator ("BCSA"), and provide his or her e-mail address, phone number, and a security device delivery address should a Hardware Digital Token device be required. Upon completion of the signing of the necessary Agreement(s) and "Company Sign-up Form", the Bank's Information Security personnel will contact your BCSA to deliver the confidential Authentication Code.

The Primary Contact person may or may not be the same as the BCSA. The Primary Contact person is to be the main contact person for general communication with the Bank. Announcements and changes with regard to Cash Management Services will be notified to the Primary Contact person by the Bank. The Primary Contact person will be responsible for liaising with the Bank and communicating such notifications to its Company's internal users.

The BCSA will be the individual security contact who accepts receipt of the IDs, security device Activation Codes, Digital Tokens or any other security device required for initial login pursuant to the Company Sign-up Form. You will notify the Bank promptly when any changes to the Primary Contact person and/or the BCSA occur – such changes include the name(s), email address(es) and phone number(s).

(c) E-Moneyger® Service Setup Procedures.

Full details of the procedures associated with the initial log-In and creation of additional User IDs for your Authorised Representatives can be found in the "E-Moneyger® System Administrator User Guide" and/or other instructions that will be provided to you by the Bank.

3. E-Moneyger® Security

(a) Protecting your Account. It is your obligation to establish and implement policies, procedures and a system of controls over the use of E-Moneyger®, 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 Representative 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 E-Moneyger® should never be left unattended whilst a session is active.

v. E-Moneyger® 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. PC's or other devices used to access E-Moneyger® 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 E-Moneyger® Services.

vii. Users should always exit the system by clicking the Logout button from the menu after using E-Moneyger®.

viii. If your BCSA, and/or Security Contacts and/or CSAs have access to the E-Moneyger® Services purely for administrative purposes, do not give them the authority to use the system to transfer funds or execute other transactions.

ix. 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. The BCSA and CSAs are responsible for instructing all Authorised Representatives 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. The BCSA and CSAs 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. For certain services (Balance and Statement Reporting, Funds Transfer Services, and Foreign Exchange & Money Market Confirmation Delivery Services), we will send an e-mail confirmation to your Primary Contact person of each user's session activity after that user has logged out of our cash management services. If a session includes funds transfers or foreign exchange & money market confirmations, confirmation of the funds transfers or foreign exchange & money market confirmations transacted during that session will be included in the Primary Contact person's e-mail confirmation. You agree that your Primary Contact person, as your representative, shall review all e-mail confirmations and shall notify us immediately if there are any discrepancies in any e-mail confirmation of a funds transfer or foreign exchange & money market confirmations (other than one relating to an employee's access level, which should be promptly reported to your Primary Contact person). The Bank provides no separate written confirmation of individual funds transfers or foreign exchange & money market confirmations conducted through our online banking

services other than the session activity e-mail confirmations sent to your Primary Contact person's e-mail address.

ii. The date and amount of transfers made through our online banking services will also be shown online under the Wire Transfer Status Reports menu, and will also be shown on your printed statements for the accounts from which the transfer is made. Additional confirmation is provided through online information available from us in electronic form as part of our online banking services and through your periodic mailed account statements. 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 your Primary Contact person). You also agree to notify us immediately of any discrepancy you may find in reviewing online information (other than one relating to an employee's access level, which should be promptly reported to your Primary Contact person).

(d) E-Moneyger® and adherence to Strong Customer Authentication (SCA)

In order to access E-Moneyger® Services you must adhere to our procedures for Secure Customer Authentication (SCA) as defined in the "Strong Customer Authentication Schedule"

4. Your Authorised Representatives

You agree that each of the Authorised Representatives (the individuals) you designate to access and use our E-Moneyger® Services are acting with your full authority in their use of these Services and in their creation and/or assignment of identifying information including Security Device Activation Codes and Digital Tokens. You further agree that all Authorised Representatives 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 E-Moneyger®. 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. Confirmation of Payee

(a) We use the Confirmation of Payee ("**CoP**") service to check the payment instruction details match those held by the bank receiving the payment. CoP applies to all single GBP payments within the UK, regardless of whether they are payments which (i) you instruct us to make for you; or (ii) we receive for your Account. We will only operate CoP with other participants who are onboarded to use CoP with Pay.UK. Please refer to "Information on Confirmation of Payee Service for E-Moneyger Customers" which we have provided to you.

(b) When you request a payment via E-Moneyger, we will use CoP to check whether the payee details match (a "**CoP Request**") and tell you the outcome of the check (the "**CoP Response**"). Where the payee details do not match or a CoP Response is not possible, we will advise you to re-confirm the payee details you have, to re-enter and submit them in a new payment instruction. We will warn you of any mismatch, that if you dismiss such warning and proceed with the payment that your funds may not reach the correct payee and that SMBC may not be able to recover the funds for you if the payment is misdirected. We will not process the payment where the CoP Response indicates that the account does not exist.

Payment Requests and Account Monitoring

(c) We are required under the CoP rules, to monitor Accounts and payments for behaviour that may indicate unusual, unlawful or wrongful activity or fraud (including behaviour contrary to anti-money laundering legislation in force from time to time), or indicate the abuse of CoP or in a manner contrary to the CoP principles or rules.

(d) Where we discover a suspected wrongful, unlawful, or illegal pattern of activity, because of our monitoring or otherwise, we are required to report this to Pay.UK and take such reasonable action as required. By using E-Moneyger to request payments for which the CoP service is provided, you understand and understand our monitoring and reporting requirements.

Right to Limit CoP Access, Freeze Accounts and Notify Pay.UK

(e) If we discover a suspected wrongful, unlawful or illegal patter of activity, whether as a result of monitoring your Account(s) or otherwise, we will report this to Pay.UK and take reasonable action as required, which may include further investigation into behaviours or use of CoP and taking remedial action such as (i) limiting your access to CoP, where we reasonably believe that you have violated the terms and conditions of CoP or acted in an unlawful manner; (ii) freezing the movement of funds, to and from your Account(s); and (iii) notifying Pay.UK of our findings.

6. Limitation of Liability

Payee Account Name – Except for where we have made an error in processing the CoP Response, we will not be responsible for misdirected payments which you have confirmed after we have warned you of the risks of proceeding where the payee account name does not match, but will use reasonable endeavours to recover such payments if they are misdirected payments. This clause does not affect payer name verification when setting up a direct debit mandate and the Direct Debit Guarantee continues to apply to those transactions.

Annex 1 - FEE ADDENDUM

This Addendum sets out our fees for providing you with our E-Moneyger® services through our corporate website, https://www.e-moneyger.com and/or https://www.smbcdigital.com. Capitalized terms used in this Addendum shall have the meaning set forth in the Cash Management Services Agreement (the "Agreement") to which you are a party.

The Fees applicable to the provision of the E-Moneyger® services to be provided by us in connection with the Agreement are as follows:

Company Name:			
Debit Account:			
Type of Fee		**Currency**	**Amount**
Initial Setup Fee			
Monthly Fees	Bank Report Service		
	Fund Transfer Service		
	Monthly Fee TOTAL		

Unless we otherwise agree in accordance with Clause 3 (*Fees*) of the Agreement, the Fees referred to above shall be payable as follows:

1. The Initial Setup Fee and the first Monthly Fees shall each be payable in arrear on the 20th day of the first calendar month falling immediately after the calendar month in which the Agreement is signed.
2. Thereafter, the Monthly Fees shall be payable in arrear on the 20th day of each calendar month during the term of the Agreement.
3. If on the date for the payment of any Fee such day is not a Business Day, then payment of the relevant Fees shall be made on the next Business Day in that calendar month (if there is one) or the preceding Business Day (if there is not).
4. All Fees shall be automatically debited from the account that you hold with us and which you agree to designate for this purpose.
5. Fees may apply for the use of “Digital Tokens” under certain circumstances.