# Cash Management Services Agreement - Strong Customer Authentication Schedule

Sumitomo Mitsui Banking Corporation DIFC Branch - Dubai

This Schedule is supplemental to the Cash Management Service Agreement (the "Agreement") between the Bank and the Customer. It defines the specific Terms and Conditions associated with the Strong Customer Authentication solutions provided by the Bank and your obligations for adherence for those Cash Management Services defined below. Expressions defined in the Agreement have the same meanings in this schedule.

## 1) Strong Customer Authentication Summary

Authentication is a procedure which allows the Bank to verify the identity of your Authorised Representative and confirm the validity of their intended use of a particular Cash Management Service.

Strong Customer Authentication (SCA) applies a higher form of authentication otherwise known as ("Two-Factor Authentication") which requires the Authorised Representative to provide authentication composed of two or more independent elements from the following categories: knowledge – something only you know, Possession – something you have, and Inherence – something you are.

Under certain circumstances, an even higher form of SCA will be applied referred to as ("Dynamic Linking") or ("Transaction Signing"). In these cases the Authorised Representative will also be asked to re-confirm details of a request submitted to ensure that this matches the details of what was received by the Bank.

The Bank continues to review and upgrade its SCA solutions inclusive of identity, session and transaction monitoring to protect you, the Bank and to align with regulatory expectations.

The Bank will rely on such SCA as the "Customer's" authority to provide access to approved third parties, allow access to account information, authorise payments from the account or other services made available to you by the Bank now or in the future.

## 2) Scope of this Schedule

(a) Service Scope. This schedule governs your obligations for SCA when using the following Cash Management Services:

I. E-Moneyger®

II. Any other service the Bank may make available to you that will rely on such authentication and authorization.

(b) Service Action. SCA can be applied by the Bank at any time and for a range of different actions but will consistently be applied when the following actions are performed:

I. Consent
II. Logon
III. Payment Approval
IV. Other approval as agreed.

**3) Strong Customer Authentication Procedures**

(a) Establishment of SCA Procedures. If required for a service, at our request you will establish appropriate SCA procedures, including the designation of Authorised Representatives to access and use the services and their use of Identifying Information, Authentication Passcodes and Digital Tokens, which they must safeguard. Using these SCA procedures you will transmit information and instructions (collectively, "Instructions") to us. We are entitled to accept and act on Instructions if they have been authenticated by the relevant SCA procedures.

(b) Purpose of SCA Procedures. SCA procedures are intended to confirm the authenticity of the Instructions you provide to us. We assume no responsibility to discover or audit any unauthorized disclosure or use of the SCA procedures or other breach of security by you, your Authorised Representatives, or any third party.

(c) Use of SCA Procedures. You acknowledge that you have been advised of the various SCA procedures employed by the Bank, that you understand them, and that the Instructions you will issue to us under the "Agreement" will employ the SCA procedure suitable to your circumstances and the Cash Management Services being accessed or used.

(d) Confidentiality of SCA Procedures. You must preserve the confidentiality of the SCA procedures both you, your Authorised Representatives and the Bank use in connection with these services. You should disclose the SCA procedures only to those Authorised Representatives who are required to know them. You must preserve the confidentiality and security of any Identifying Information, Authentication Passcodes, Digital Tokens or other any other security devices and make them available only to the authorised individuals designated by you to use the Services.

**4) Digital Tokens**

4.1) To facilitate your interaction with SCA, the Bank will provide a Digital Token for each Authorised Representative which allows them to:

(a) Activate the token by receiving activation information from the Bank and setting up Identifying Information and Authentication Passcodes on the device
(b) Authenticate into the online cash management services provided by the Bank to you (as defined in section 2a)
(c) Sign payment transactions you have initiated from your accounts held with the Bank using these Cash Management Services (as defined in section 2a)

4.2) The Digital Token is purely for user authentication and transaction signing. It does not offer other banking services such as account reporting or payment initiation.

4.3) The Digital Token is provided as part of our service to you and is solely for the use of your Authorised Representatives. The Digital Token is not designed or intended for and should not be downloaded or used by, individuals or consumers acting in their own capacity.

4.4) We will protect the communication sessions between you and us as part of the SCA Service using the Digital Token against the capture of authentication data transmitted during the authentication, and against manipulation by unauthorised parties.

4.5) You will notify the Bank immediately if you have received information on a Digital Token that is not meant for you.

4.6) You will notify the Bank immediately if you know or believe any of your Identifying Information, Authentication Passcodes or Digital Tokens have been compromised in some way.

4.7) You will follow all security measures and advices provided by the Bank.

4.8) We do not guarantee that the Digital Token will always be available and functional. If you are unable to use the Digital Token and therefore cannot access the Bank's Cash Management Services because the Digital Token or associated services provided are unavailable or interrupted we shall have no liability to you.

4.9) By entering the Agreement, you agree to the licence and liability terms, as listed in Appendix 1 to this Schedule, relating to the Mobile Authenticator App.

## 5) The right to suspend SCA Services

5.1) We may suspend or withdraw or restrict at any time the availability of all or any part of the SCA Service and the Digital Token for security, operational, legal or business reasons. We will try to give you reasonable notice of any suspension.

5.2) Access to the Digital Token will be suspended if your Authorised Representative enters incorrect authentication details repeatedly.

## 6) The right to terminate SCA Services

6.1) We can terminate this Schedule or stop providing the SCA Service through the Digital Token at any time and for any reason. We may also change, suspend, terminate or discontinue any aspect of the SCA Service including availability of certain features at any time and for any reason. Where possible we will endeavor to give you notice before doing so.

6.2) You can terminate this Schedule insofar as they are applicable to you for any reason by giving us immediate notice. In addition, either party may terminate this Schedule immediately if the other is breaching any of its responsibilities under this Schedule.

6.3) On any termination of this Schedule, your right and those of your Authorised Representatives to access the SCA Service through the Digital Token will cease and we may terminate your access to the SCA Service through the Digital Token and invalidate all or any relevant access details to the Digital Token.

6.4) Termination for whatever reason of this Schedule will not affect (a) any rights, liabilities or obligations which accrued before such termination; or (b) any of this Schedule that is intended to continue to have effect after such termination.

## 7) Personal Information

The personal information your Authorised Representative submits to the Bank and that the Bank collects in connection with their use of the Digital Token and/or SCA Service is governed by our Website Terms of Use and Privacy Notice. To the extent there is an inconsistency relating to personal information between these Terms and the Website Terms of Use and Privacy Policy, the terms of the Website Terms of Use and Privacy Policy shall prevail.
https://www.smbcgroup.com/emea/about-us/customer-information-and-notices/#privacy

**8) Responsibilities**

8.1) Nothing in these Terms excludes our liability for death or personal injury arising from our negligence, or our fraud or fraudulent misrepresentation, or any other liability that cannot be excluded or limited by the laws of the DIFC or other applicable law.

8.2) To the maximum extent permitted by applicable law, we exclude all conditions, warranties, representation or other terms which may apply to the Digital Token, whether express or implied. The Digital Token is provided "as is" with no representation, guarantee or agreement of any kind as to its functionality.

8.3) To the maximum extent permitted by applicable law, the Bank shall not be liable to you for any loss or damage, whether in contract, tort (including negligence), breach of statutory duty, or otherwise, even if foreseeable, arising under or in connection with the use of, or inability to use, the Digital Token.

8.4) Without prejudice to the Banking Terms, the Bank shall not be liable for any loss of profit, loss of sales, transactions or business, loss of agreements or contracts, loss of use or corruption of software, data or information, any indirect, consequential, incidental, punitive, exemplary or special losses or damages, or expenses (including without limitation attorneys' fees), which you may incur or suffer including, without limitation, any loss, damage or expense from subsequent dishonour or rejection of any transaction, whether or not the possibility or likelihood of such damage was known or contemplated by us.

**APPENDIX 1. Mobile Authenticator App Licence and Liability Terms**

1 **LICENCE TERMS**

1.1 The Bank grants to you a limited, non-exclusive, revocable, non-transferable (except as otherwise permitted in this Clause 1) licence to install and use the Mobile Authenticator App on Android or iOS phones controlled by you (the "**Licensed Equipment**"), subject to the terms of the Agreement. This Licence shall be terminated on the expiry or termination of the Agreement or Strong Customer Authentication Schedule.

1.2 You shall not, nor permit others to:

(a) use or copy the Mobile Authenticator App except as expressly permitted in the Agreement or applicable law;

(b) translate, reverse engineer, decompile, disassemble or attempt to derive the source code or object code of the Mobile Authenticator App, except to the extent expressly permitted by applicable mandatory law;

(c) rent, lease, assign or otherwise transfer the Mobile Authenticator App and/or activation codes except as expressly agreed in writing;

(d) modify the Mobile Authenticator App or merge all or any part of the Mobile Authenticator App with any unauthorised program, unless such use is approved by the Bank in writing;

(e) modify or delete any copyright, trademark, other proprietary rights notice on the Mobile Authenticator App or other documentation related to the Mobile Authenticator App;

(f) copy, except to the extent permitted in the Agreement or applicable law, any documentation related to the Mobile Authenticator App without reproducing applicable copyright, trademark or proprietary rights notices on each copy;

(g) impair in any way the Bank or the Bank's licensor's copyright, trademark or other proprietary rights;

(h) use, copy, modify or create new activation codes unless expressly permitted in the Agreement;

(i) use or allow the use of the Mobile Authenticator App in violation of U.S., European or other applicable export regulations, or for any other unlawful activity or in any unauthorised manner;

(j) download or install the Mobile Authenticator App onto a jail-broken or rooted mobile device;

(k) tamper with the Mobile Authenticator App or otherwise use the Mobile Authenticator App in a way that could damage it or stop it from working or affect the systems, such as hacking into or inserting malicious codes into the Mobile Authenticator App or mobile operating systems;

(l) use the Mobile Authenticator App in a way that could damage, disable, overburden, impair or compromise our systems or security or interfere with other users of the Mobile Authenticator App; or

(m) collect or harvest any information from the Mobile Authenticator App or our systems or attempt to decipher any transmissions to or from the servers running the Mobile Authenticator App or our systems.

1.3 You must:

(a) only use the Mobile Authenticator App, and procure that the use by any Authorised Representatives shall be, in accordance with the terms of the Agreement, and the end user licence agreement, as annexed to this Schedule, and as may be amended or presented to Authorised Representatives from time to time (the "**Mobile Authenticator App Terms**");

(b) only allow your Authorised Representatives to use the Mobile Authenticator App, and procure that they do so solely in connection with the administration of the Services for your business purposes;

(c) have provided the Bank with accurate, current and complete details of Authorised Representatives as that are necessary for the Bank to provide the Mobile Authenticator App, and you shall keep such information accurate, current and complete;

(d) comply with, and procure that the Authorised Representatives comply with, the terms of the Agreement and the Mobile Authenticator App Terms;

(e) implement and maintain procedures to ensure that you are able to monitor compliance with the terms of the Agreement and the Mobile Authenticator App Terms;

(f) only use the Mobile Authenticator App, and procure that use by any Authorised Representatives shall be, in compliance with all applicable laws, including any consumer, data protection, data privacy and export control laws; and

(g) update or procure the update of the operating systems of Licensed Equipment if advised by the Bank that this is necessary for security reasons.

1.4 The Bank can terminate or stop providing, suspend, withdraw, or restrict the Mobile Authenticator App or your licence to install and use it at any time and for any reason. The Bank may also change, suspend, terminate or discontinue any aspect of the Mobile Authenticator App including availability of certain features at any time and for any reason. Where possible the Bank will endeavour to give you notice before doing so.

1.5 If Authorised Representatives enter incorrect authentication details repeatedly, access to the Mobile Authenticator App will be suspended. You must contact your system administrator or the Bank's help desk for further support.

1.6 The Mobile Authenticator App has not been developed to meet your individual requirements. You are responsible for ensuring that the facilities and functions of the Mobile Authenticator App meet your requirements.

1.7 All intellectual property rights in the Mobile Authenticator App throughout the world belong to the Bank (or its licensors) and the rights in the Mobile Authenticator App are licensed (not sold) to you. You have no intellectual property rights in, or to the Mobile Authenticator App other than the right to use them in accordance with the terms of the Agreement.

1.8 As set out in Clause 1.2, you must not infringe the Bank's intellectual property rights or those of any third party (including the Bank's licensors) in relation to your use of the Mobile Authenticator App.

2 **LICENCE LIABILITY**

2.1 Nothing in this Clause 2 excludes the Bank's liability for death or personal injury arising from our negligence, or the Bank's fraud or fraudulent misrepresentation, or any other liability that cannot be excluded or limited by the laws of the DIFC or other applicable law.

2.2 To the maximum extent permitted by applicable law, the Bank excludes all conditions, warranties, representations or other terms which may apply to the Mobile Authenticator App, whether express or implied. The Mobile Authenticator App is provided "as is" with no representation, guarantee or agreement of any kind as to its functionality or availability.

2.3 The Bank does not guarantee that the Mobile Authenticator App will always be available or be uninterrupted.

2.4 The Bank shall not be liable to you for any loss or damage, whether in contract, tort (including negligence), breach of statutory duty or otherwise, even if foreseeable, arising under or in connection with the use of, or inability to use, the Mobile Authenticator App.

2.5 In relation to the use of, or inability to use, the Mobile Authenticator App, the Bank shall not be liable for any loss of profit, loss of sales, transactions or business, loss of agreements or contracts, loss of use or corruption of software, data or information, any indirect, consequential, incidental, punitive, exemplary or special losses or damages or expenses (including without limitation attorneys' fees), which you may incur or suffer including, without limitation, any loss, damage or expense from subsequent dishonour or rejection of any transaction, whether or not the possibility or likelihood of such damage was known or contemplated by us.

2.6 You agree to defend, indemnify and hold the Bank free and harmless from any claim and against any loss or damage which the Bank may suffer or incur as a result of your (and your Authorised Representatives) use of the Mobile Authenticator App or any breach of your obligations set out in Clause 1 (Licence Terms).