



MUFG Exchange Supplement

EFFECTIVE JANUARY 1, 2025

This MUFG Exchange Supplement (“**Supplement**”) is a part of and is to be read together with either the Deposit Accounts & Services Disclosure Agreement (“**Deposit Agreement**”) or the Master Terms of Business for Banking (“**Master Terms of Business**”). The Deposit Agreement and/or Master Terms of Business, each as may be amended or supplemented, are hereinafter referred to as the Account Agreement. Capitalized words used in this Supplement and not defined herein have the meanings ascribed to them in the Account Agreement. In the event of any inconsistency between this Supplement and the Account Agreement, this Supplement shall govern for the purpose of MUFG Exchange.

MUFG EXCHANGE SERVICE

The Bank will provide a Service that enables electronic access to certain cash management services via the MUFG Exchange web and mobile channels. MUFG Exchange enables the Customer to electronically: i) access Account information, reports, statements, and data; ii) issue transactions, inquiries, or instructions (payment or nonpayment); and/or iii) transmit and receive notifications and alerts. The Customer will have the ability to electronically administer users and manage entitlements, as further described below.

ACCESS TO SERVICES

The Services accessible via MUFG Exchange are further described in the Account Agreement, including the Transaction Banking Services Supplement, as applicable. Access to Services via MUFG Exchange requires users to have the appropriate entitlements. Users that access MUFG Exchange via mobile will have access to some (but not all) Services available via MUFG Exchange web.

By executing the Bank’s authorization and agreement form, the Customer agrees to be bound by the terms of this Supplement. The Bank will provide the Customer with procedures, user guides, and specifications (collectively, “**User Guides**”) for use of MUFG Exchange. The Customer agrees to comply with the User Guides that the Bank makes available to the Customer. The Customer is responsible for all actions taken by its users of MUFG Exchange.

SECURITY PROCEDURE AND ADMINISTRATIVE CONTROLS

a. **Security Procedure.** The Security Procedure for access to MUFG Exchange via web and mobile and for releasing payment instructions thereunder is a password, user identification code, and a token code generated by an approved security device (collectively “**Credentials**”). Access to MUFG Exchange using Credentials will be deemed to have been authorized by the Customer. Any payment instruction, the authenticity of which has been verified through use of the Credentials, shall be effective as that of the Customer, whether or not authorized. It is understood that the purpose of the security procedure is to verify the authenticity of, and not to detect errors in, instructions. The Customer further agrees that this security procedure best meets its needs given the size, type, and frequency of payment transactions, and is a commercially reasonable security procedure for the Customer.

The Customer is responsible for the confidentiality and use of the Credentials. Credentials are intended for use on a single user basis only and should not be shared. The Customer agrees to safeguard the Credentials, and to instruct all Security Administrators and users to do the same. The Customer shall notify the Bank immediately of loss or theft of Credentials, any unauthorized use of the Credentials, or any other breach of security. The Bank may suspend or disable any Credential if, in its sole discretion, the Bank has reason to suspect improper use of the Service or Credentials, and/or for security reasons. Administrative controls and procedures (identified below in Section b) and unilateral Bank controls shall not be deemed to be a security procedure for purposes hereof unless explicitly identified as such in writing.

b. **Administrative Procedures and Controls.** The Bank offers numerous additional controls that the Customer may implement to enhance security and reduce the risk of erroneous or unauthorized transactions. These procedures and controls may include, among others, IP address restrictions, Account and transaction payment limits, and notification of certain administration changes, each as are further described in the User Guides, and which may be supplemented and modified by the Bank from time to time. The application of the Security Procedure, administrative controls, the Bank’s unilateral controls and dual control for payment, payment templates and Administration approval may cause delays in processing of instructions, result in the Bank denying access to MUFG Exchange or Service, and/or the Bank’s declining to execute an instruction.

MUFG Bank, Ltd.

A member of MUFG, a global financial group

- c. **Security Administrator Designation.** The Customer shall designate and notify the Bank of a minimum of two administrators (each a “**Security Administrator**”) who have equal authority in accordance with the administrative control procedure for accessing MUFG Exchange. The Customer agrees to notify the Bank of any change in Security Administrators in the manner and form designated by the Bank. Any such change shall be effective at such time as the Bank has received such notice and has had reasonable opportunity to act upon it. The Customer assumes sole responsibility for the actions of its Security Administrators, the entitlements assigned to users, and the actions of the users to access MUFG Exchange and the Services. The Customer is responsible for ensuring Security Administrators, users, and entitlements remain current.

Unless otherwise set forth in the Transaction Banking Service Supplement, the Security Administrators shall be responsible for: (i) designating individuals as users; (ii) designating additional Security Administrators; (iii) assigning, removing, and/or approving the Service(s) that each user may access; (iv) assigning, removing, and/or approving user entitlements and Accounts that each user may access; and (v) advising each user of his/her obligations hereunder or under any the applicable documentation. The Security Administrator shall also be responsible for disseminating and activating tokens and advising each user of his/her responsibilities and obligations under the Account Agreement as supplemented by this MUFG Exchange Supplement. At regular intervals, to reduce security risk of users designated as “inactive”, the Bank may de-activate tokens and delete users who have not accessed MUFG Exchange for thirteen consecutive months and/or any user who fails to access the Service after ninety days from initial creation.

OPEN NETWORK ACCESS; INTERNAL SECURITY

The Customer is responsible for obtaining and maintaining equipment that is necessary for the Customer to use MUFG Exchange, such as hardware, telecommunication equipment, Internet connections, and web browser software or other equipment (collectively, “**Systems**”). MUFG Exchange must be accessed in accordance with the Bank’s recommended system configurations, and the Bank disclaims all risks relating thereto, and makes no endorsement thereof, notwithstanding that the Bank may recommend certain Systems. The Customer agrees to at all times maintain current and effective anti-virus and anti-spyware software and shall take all reasonable measures to maintain the security of the Customer’s Systems. The Bank is not responsible for the unavailability or temporary interruption of the Service due to service issues, Systems issues, lack of network coverage, or technical failure of the mobile device or wireless service provider. The Customer acknowledges that there are certain security, corruption, transmission error, and access availability risks associated with using open networks such as the Internet. MUFG Exchange is made available “as-is” and “as available.” To the maximum extent permitted under applicable law, all warranties, including implied warranties of merchantability and fitness for a particular purpose, are expressly disclaimed. The Customer further acknowledges that it has made an independent assessment of the adequacy of the Internet and the Systems in connection with the use of MUFG Exchange.

ALERTS; DATA; INSTRUCTIONS

The Customer may access MUFG Exchange to obtain balance, transaction, and other Account information and, upon Customer’s request, information regarding third party bank accounts or other third-party information. The Customer acknowledges that data and information may be periodically updated and adjusted. The Customer authorizes the Bank to send and, as applicable, receive data, message notifications and alerts through any communication service providers, including both Internet and telecommunications providers, which shall each be deemed to be acting as the Customer’s agent. Such providers may not encrypt communications. The Customer shall be responsible for the accuracy of all data, information, and instructions received by the Bank via MUFG Exchange, including, without limitation, information received from third parties. Further, the Bank shall have no liability for the receipt or viewing by any party of data sent to the destinations designated by the Customer including but not limited to email addresses, fax and telephone number(s).

Access to MUFG Exchange via mobile is provided at no additional cost. However, users may incur charges for mobile Internet access and should contact their wireless carrier for more information.

WARRANTIES

The Customer represents and warrants to the Bank that it will not, nor will it allow any third party to, use MUFG Exchange in any manner whatsoever that violates, causes the Bank to violate, or is otherwise contrary to any laws or regulations concerning money laundering and terrorist financing, economic trade, or other sanction law, including, but not limited to, those administered by the U.S. Treasury Department’s Office of Foreign Assets Control. The Customer represents and warrants to the Bank that the Customer shall not use MUFG Exchange while located in a country or territory targeted by comprehensive, country-wide or territory-wide sanctions (such countries or territories, hereinafter referred to as “**Sanctioned Jurisdiction**”). Any attempt to access from Sanctioned Jurisdiction may constitute a breach of this Supplement and could potentially subject the Customer to penalties by U.S. authorities. The Customer further represents and warrants to the Bank that prior to submitting any document(s) that identifies Security Administrators or users (whether electronically or via a set-up form), the Customer shall have obtained from each individual referred to in such document all necessary consents to enable and authorize the Bank to send alerts/notifications and to process the data for the purpose of providing access to MUFG Exchange and/or a Service.

MISCELLANEOUS

Except as specifically set forth in this Supplement, all terms and conditions in the Account Agreement, including but not limited to the terms and conditions related to liability, fees, indemnification, termination, and dispute resolution, remain in full force and effect and apply to the Customer’s use of MUFG Exchange.