TÉRMINOS DE SERVICIO DE CANALES ELECTRÓNICOS PARA SERVICIOS DE TESORERÍA J.P. MORGAN

J.P. MORGAN TREASURY SERVICES ELECTRONIC CHANNELS SERVICE TERMS[1]

1. Servicio y Términos de Servicio.

El Banco proporcionará un servicio (el "**Servicio**") para el acceso electrónico a la información, informes y datos de la cuenta del Cliente (en conjunto, los "**Datos**") y para la transmisión electrónica al Banco de mensajes, solicitudes de servicio e instrucciones de pago y de no pago (cada una, una "Instrucción"), y del Banco, de mensajes, notificaciones y alertas, a través de J.P. Morgan Access® Online, J.P. Morgan Access® Mobile, J.P. Morgan Host-to-Host/transferencia de archivos administrados y de los canales API de los Servicios de Tesorería J.P. Morgan. El Banco se reserva el derecho de modificar las aplicaciones y los productos disponibles a través del Servicio. El Servicio se rige por estos términos (los "**Términos del Servicio**"), que incorporan los términos del Banco que rigen las cuentas y los servicios comerciales, incluidos los términos del servicio que rigen el procesamiento por parte del Banco de las Instrucciones transmitidas a través del Servicio (en conjunto, la "**Documentación de la Cuenta**"), ya que el mismo puede ser modificado periódicamente. En caso de que exista un conflicto entre la Documentación de la Cuenta y los presentes Términos de Servicio, y en la medida en que exista, prevalecerán las disposiciones de estos Términos de Servicio. Los términos en mayúsculas utilizados en estos Términos de Servicio, y no definidos de otra manera, tienen el significado establecido en los Términos Globales de la Cuenta u otros términos de la cuenta aplicables al Cliente. JPMorgan Chase Bank, N.A. está organizado bajo las leyes de EE.UU., con responsabilidad limitada.

1. Service and Service Terms.

The Bank will provide a service (the "**Service**") for electronic access to the Customer's account information, reports and data (collectively, "**Data**") and for the electronic transmission to the Bank of messages, service requests, and payment and non-payment instructions (each an "**Instruction**") and from the Bank of messages, notifications and alerts, via the J.P. Morgan Access® Online, J.P. Morgan Access® Mobile, J.P. Morgan Host-to-Host/managed file transfer and J.P. Morgan Treasury Services API channels. The Bank reserves the right to modify the applications and products available via the Service. The Service is governed by these terms (the "**Service Terms**"), which incorporate the Bank's terms governing the business accounts and services, including service terms that govern the Bank's processing of Instructions transmitted via the Service (collectively, the "**Account Documentation**"), as the same may be amended from time to time. If and to the extent that there is a conflict between the Account Documentation and these Service Terms, the provisions of these Service Terms shall prevail. Capitalized terms used in these Service Terms, and not otherwise defined, have the meaning set forth in the Global Account Terms or other account terms applicable to the Customer. JPMorgan Chase Bank, N.A. is organized under the laws of U.S.A. with limited liability.

2. Procedimientos de Seguridad y Otros Controles

2.1 General. Los procedimientos de seguridad para cada canal se establecen a continuación, mismos que pueden ser modificados mediante una notificación al Cliente a través de cualquier medio (cada uno, un "**Procedimiento de Seguridad**"). Cualquier Instrucción cuya autenticidad haya sido verificada a través de un Procedimiento de Seguridad, será efectiva como la del Cliente, esté o no autorizada, y no obstante la Instrucción pueda provocar un sobregiro de una Cuenta. Los controles implementados unilateralmente por el Banco no se considerarán Procedimientos de Seguridad para los fines del presente, a menos que se identifiquen explícitamente como tales por escrito. El Cliente es responsable de implementar los procedimientos y requisitos establecidos en la documentación aplicable que le proporcione el Banco, así como cualquier modificación posterior a los procedimientos y requisitos que están diseñados para fortalecer los Procedimientos de Seguridad.

2.2 Procedimientos de Seguridad y Otros Controles para Access En Línea y Canales Móviles.

2.2.1 Access En Línea. El Procedimiento de seguridad para verificar las Instrucciones de pago que se dan a nombre del Cliente a través del canal Access Online es la validación de una identificación de usuario y una contraseña confidencial de un Usuario autorizado (como se define en la Sección 2.6 a continuación), un código de token generado por un dispositivo de seguridad emitido o aprobado por el Banco (que incluye software y hardware utilizados para generar "soft tokens" en un dispositivo móvil) ("**Dispositivo de Seguridad**") asignado a ese Usuario Autorizado y revisión de la transacción bancaria, tal como se especifica en la Sección 2.5.

2. Security Procedures and Other Controls

2.1. General. The security procedures for each channel are set forth below, as may be modified on notice to the Customer through any medium (each, a "**Security Procedure**"). Any Instruction, the authenticity of which has been verified through a Security Procedure, shall be effective as that of the Customer, whether or not authorized, and notwithstanding that the Instruction may result in an overdraft of an Account. Controls unilaterally implemented by the Bank shall not be deemed to be Security Procedures for purposes hereof unless explicitly identified as such in writing. The Customer is responsible for implementing any procedures and requirements set forth in the applicable documentation provided to it by the Bank, as well as any subsequent modification to the procedures and requirements that are designed to strengthen the Security Procedures.

2.2. Security Procedures and Other Controls for Access Online and Mobile Channels.

2.2.1. Access Online. The Security Procedure for verifying payment Instructions given in the Customer's name via the Access Online channel is validation of a user ID and confidential password of an Authorized User (as defined in Section 2.6 below), validation of a token code generated by a Bank issued or approved security device (which, for the avoidance of doubt, includes software and hardware used to generate "soft tokens" on a mobile device) ("**Security Device**") assigned to that Authorized User and Bank transaction review as specified in Section 2.5.

2.2.2 Access Mobile. El Procedimiento de Seguridad para verificar las Instrucciones de pago dadas a nombre del Cliente a través del canal Access Mobile es (i) la validación del registro con el Banco del dispositivo móvil utilizado en la transacción, verificación biométrica de la identidad del Usuario Autorizado mediante un método emitido o aprobado por el Banco, la introducción de un PIN adjunto de un Usuario Autorizado (según se define en la Sección 2.6 a continuación) y la revisión de la transacción según se especifica en la Sección 2.5; (ii) validación de una ID de usuario y contraseña confidencial de un Usuario Autorizado (según se define en la Sección 2.6 a continuación), un código de token generado por un Dispositivo de Seguridad asignado a ese Usuario Autorizado y revisión de transacciones como se especifica en la Sección 2.5 o una combinación de tres o más factores en (i) y (ii).

2.2.3 Controles Ofrecidos al Cliente. Para el Access en Línea y Móvil, el Cliente puede optar por aplicar ciertos controles periódicamente ofrecidos por el Banco al Cliente, diseñados para reducir el riesgo del Cliente de transacciones no autorizadas. El Cliente es responsable de elegir los controles que sean apropiados para el Cliente mismo, teniendo en cuenta, entre otras cosas, la naturaleza y la escala del negocio del Cliente, incluido el tamaño, el tipo y la frecuencia de las órdenes de pago normalmente emitidas al Banco, y la naturaleza de su entorno técnico, controles contables internos y políticas y procedimientos de seguridad de la información (en conjunto, "**Controles Internos del Cliente**"). El Procedimiento de Seguridad que se establece por acuerdo entre el Cliente y el Banco en el presente documento, se establece en vista de los Controles Internos del Cliente aplicados por el Cliente. Para evitar dudas, ninguno de los controles descritos en esta Sección forman parte de los Procedimientos de Seguridad para los canales.

2.3 Procedimientos de Seguridad y Procedimientos de Certificado para el Canal de Transferencia de Archivos de Host a Host/Administrado. El Procedimiento de Seguridad para verificar las Instrucciones de pago que se dan a nombre del Cliente a través del canal de transferencia de archivos Host a Host/administrado es la autenticación de un certificado de firma digital, que autentica los archivos transmitidos sobre la base de la clave de seguridad correspondiente (el "**Certificado de Firma**") y la revisión de transacciones según lo dispuesto en la Sección 2.5. El Cliente y el Banco utilizarán los siguientes procedimientos para el uso de un certificado de transporte, que establece una sesión segura entre el Banco y el Cliente sobre la base de una clave de seguridad correspondiente (el "**Certificado de Transporte**") y el Certificado de Firma. Cada uno de los Certificados de Firma y el Certificado de Transporte se denominan en este documento como un "**Certificado**" y la clave de seguridad correspondiente como una "**Clave de Seguridad**".

2.3.1 Procedimientos y Requerimientos del Certificado. El Cliente deberá cumplir con los procedimientos y requisitos del Banco para Certificados y Claves de Seguridad notificados al Cliente, incluidos, entre otros, el período de validez del Certificado, la solidez de la clave y las especificaciones criptográficas, según se modifiquen periódicamente. Cualquier solicitud al Banco para agregar, actualizar o eliminar una Clave de Seguridad deberá incluir el Certificado correspondiente, un archivo de texto u otra representación física de la Clave de Seguridad

2.2.2. Access Mobile. The Security Procedure for verifying payment Instructions given in the Customer's name via the Access Mobile channel is (i) validation of the registration with the Bank of the mobile device used in the transaction, biometric identity verification of the Authorized User by a Bank-issued or approved method, entry of an accompanying PIN of an Authorized User (as defined in Section 2.6 below) and transaction review as specified in Section 2.5; (ii) validation of a user ID and confidential password of an Authorized User (as defined in Section 2.6 below), a token code generated by a Security Device assigned to that Authorized User and transaction review as specified in Section 2.5 or a combination of three or more factors in (i) and (ii).

2.2.3. Controls Offered to Customer. For Access Online and Mobile, the Customer may choose to apply certain controls offered by the Bank to the Customer from time to time designed to reduce the Customer's risk of unauthorized transactions. The Customer is responsible for choosing controls that are appropriate for the Customer taking into account, among other things, the nature and scale of the Customer's business, including the size, type and frequency of payment orders normally issued to the Bank, and the nature of its technical environment, internal accounting controls and information security policies and procedures (collectively, "**Customer Internal Controls**"). The Security Procedure that is established by agreement of the Customer and the Bank herein is established in view of the Customer Internal Controls applied by the Customer. For the avoidance of doubt, none of the controls described in this Section are part of the Security Procedures for the channels.

2.3. Security Procedures and Certificate Procedures for Host-to-Host/Managed File Transfer Channel. The Security Procedure for verifying payment Instructions given in the Customer's name via the Host-to-Host/managed file transfer channel is authentication of a digital signature certificate, which authenticates transmitted files on the basis of the corresponding security key (the "**Signature Certificate**") and transaction review as provided in Section 2.5. The Customer and the Bank will use the following procedures for the use of a transport certificate, which establishes a secure session between the Bank and the Customer on the basis of a corresponding security key (the "**Transport Certificate**") and the Signature Certificate. Each of the Signature Certificate and the Transport Certificate are referred to herein as a "**Certificate**" and the corresponding security key as a "**Security Key**".

2.3.1. Certificate Procedures and Requirements. The Customer shall comply with the Bank's procedures and requirements for Certificates and Security Keys notified to the Customer, including but not limited to Certificate validity period, key strength and cryptographic specifications, as amended from time to time. Any request to the Bank to add, update or delete a Security Key shall include the applicable Certificate, a text file or other physical representation of the public Security Key of such Certificate and any other information in the manner and form designated by the Bank. The Bank shall

[1] *The English version of this document is included only for reference purposes. Any inconsistencies with the Spanish version shall be interpreted as it is understood in Spanish.*

pública de dicho Certificado y cualquier otra información en la manera y forma que designe el Banco. El Banco tendrá derecho a basarse en cualquier solicitud que el Banco crea de buena fe que haya sido enviada por el administrador de seguridad designado ("**Administrador de Seguridad**"), sin prejuicio de que dicho Administrador de Seguridad pueda ser un tercero que actúe en nombre del Cliente.

2.3.2 Caducidad del Certificado. No obstante las notificaciones de cortesía que el Banco pueda enviar al Cliente con respecto al vencimiento inminente del Certificado del Cliente, el Cliente reconoce que es responsabilidad exclusiva del Cliente actualizar el Certificado antes de su fecha de vencimiento. El Banco no será responsable de ninguna pérdida o daño (incluido, para evitar dudas, cualquier daño o pérdida indirecto, especial, punitivo o consecuente) que surja de la falta de actualización oportuna del Certificado por parte del Cliente. Para permitir la ejecución adecuada de los procedimientos administrativos y evitar cualquier lapso en el servicio o procedimientos de emergencia, el Cliente debe solicitar un cambio de Certificado al menos 30 días antes de la expiración real del Certificado.

2.4 Procedimiento de Seguridad y Procedimientos del Certificado/Token para el Canal API. El Procedimiento de Seguridad para verificar las Instrucciones de pago que se dan a nombre del Cliente a través del canal API es la autenticación de un Certificado de Firma y la revisión de la transacción, tal como se indica en la Sección 2.5.

2.4.1 Sesión Segura. El Cliente y el Banco establecerán una sesión segura entre el Cliente y el Banco mediante la validación de (i) un Certificado de Transporte o (ii) un token generado por el Banco ("**Token API**").

2.4.2 Procedimientos y Requisitos del Certificado. El Cliente y el Banco utilizarán los procedimientos establecidos en las Secciones 2.3.1 y 2.3.2 para el uso de los Certificados para el canal API.

2.4.3 Procedimientos y Requisitos del Token API. El Cliente deberá cumplir con los procedimientos y requisitos del Banco para los Tokens API, según se modifiquen periódicamente, lo cual incluye, entre otros, la generación y custodia de cualquier credencial utilizada para la validación del Token API, notificada al Cliente. El Banco tendrá el derecho de revocar un Token API en cualquier momento, incluso en base a una solicitud o comunicación relacionada con un Token API que el Banco crea que de buena fe haya sido enviada por el Administrador de Seguridad, sin perjuicio de que dicho Administrador de Seguridad pueda ser un tercero que actúe a nombre del Cliente. Cualquier solicitud al Banco para actualizar un Token API se realizará únicamente en la manera y forma designada por el Banco.

2.5 Revisión de Transacciones. Además de los Procedimientos de Seguridad descritos anteriormente, el Procedimiento de Seguridad aplicable para cada canal también incluye la revisión de transacciones basada en varias características de riesgo. La revisión de la transacción se llevará a cabo de acuerdo con los protocolos comercialmente razonables seleccionados por el Banco. Es posible que se requiera autenticación adicional del Cliente, por ejemplo, como una verificación de devolución de llamada, para completar ciertas transacciones identificadas por el Banco a través de la revisión de transacciones.

have the right to rely on any request that the Bank believes in good faith to have been sent by the designated security administrator ("**Security Administrator**"), notwithstanding that such Security Administrator may be a third party acting on behalf of the Customer.

2.3.2. Certificate Expiration. Notwithstanding any courtesy notifications the Bank may send to the Customer regarding the Customer's impending Certificate expiration, the Customer acknowledges that it is the Customer's sole responsibility to update the Certificate prior to its expiration date. The Bank shall have no liability for any loss or damage (including, for the avoidance of doubt, any indirect, special, punitive or consequential damages or losses) arising from the Customer's failure to timely update its Certificate. To allow for proper execution of administrative procedures, and to prevent any lapse in service or emergency procedures, the Customer must request a Certificate change at least 30 days prior to actual Certificate expiration.

2.4. Security Procedure and Certificate/Token Procedures for API Channel. The Security Procedure for verifying payment Instructions given in the Customer's name via the API channel is authentication of a Signature Certificate and transaction review as provided in Section 2.5.

2.4.1. Secure Session. The Customer and the Bank will establish a secure session between the Customer and the Bank by validation of either (i) a Transport Certificate or (ii) a Bank-generated token ("**API Token**").

2.4.2. Certificate Procedures and Requirements. The Customer and the Bank will use the procedures set forth in Sections 2.3.1 and 2.3.2 for the use of Certificates for the API channel.

2.4.3. API Token Procedures and Requirements. The Customer shall comply with the Bank's procedures and requirements for API Tokens, as amended from time to time, including but not limited to the generation and safekeeping of any credentials used for the validation of the API Token, notified to the Customer. The Bank shall have the right to revoke an API Token at any time, including in reliance on a request or communication related to an API Token that the Bank believes in good faith to have been sent by the Security Administrator, notwithstanding that such Security Administrator may be a third party acting on behalf of Customer. Any request to the Bank to update an API Token shall be made solely in the manner and form designated by the Bank.

2.5. Transaction Review. In addition to the Security Procedures described above, the applicable Security Procedure for each channel also includes transaction review based on various risk characteristics. The transaction review shall be conducted in accordance with commercially reasonable protocols selected by the Bank. Additional authentication from the Customer, such as call-back verification, may be required to complete certain transactions identified by the Bank through transaction review.

2.6 **Violación de Confidencialidad/Seguridad.** El Cliente será responsable de salvaguardar y garantizar que los Procedimientos de Seguridad, los Dispositivos de Seguridad, los Tokens API y cualquier credencial utilizada para la validación del Token API sean conocidos y utilizados (i) en el caso de Access En Línea y Móvil, solamente por personas designadas como usuarios por los Administradores de Seguridad ("**Usuarios Autorizados**"), o bien, (ii) en el caso de la transferencia de archivos de Host a Host/administrados y canales API, únicamente por los Administradores de Seguridad, según corresponda. El Cliente notificará de inmediato al Banco en caso de pérdida, robo o uso no autorizado de un Procedimiento de Seguridad, un Dispositivo de Seguridad, el Token API, cualquier credencial utilizada para la validación del Token API o cualquier otra violación de seguridad. El Banco puede deshonrar o deshabilitar cualquier Dispositivo de Seguridad, Token API, cualquier credencial utilizada para la validación del Token API o cualquier aspecto de los Procedimientos de Seguridad en cualquier momento, sin previo aviso, e informará al Cliente de lo mismo. Además, cada Cliente debe implementar su propia seguridad física y lógica, así como controles de administración, que protejan adecuadamente el hardware, el software y los controles de acceso utilizados en el proceso de transacción frente al acceso y uso no autorizados.

2.7 **Designación del Administrador de Seguridad**. El Cliente designará Administradores de Seguridad quienes tendrán la misma autoridad que se especifica en la Sección 2.8 a continuación. El Banco tiene el derecho de confiar en dicha designación de un Administrador de Seguridad. El Cliente se compromete a notificar al Banco de cualquier cambio en los Administradores de Seguridad en la manera y forma designada por el Banco. Cualquier cambio será efectivo en el momento en que el Banco haya recibido dicha notificación y haya tenido una oportunidad razonable para actuar en consecuencia.

2.8 **Responsabilidades del Administrador de Seguridad**. Cada Administrador de Seguridad estará autorizado por el Cliente y será responsable de (i) designar personas como Usuarios Autorizados con respecto a los canales de Access En Línea y Móvil; (ii) identificar las funciones del Servicio a las que cada Usuario Autorizado puede acceder; (iii) solicitar, crear, controlar, difundir y/o cancelar los derechos de los usuarios con respecto a los canales Access En Línea y Móvil; (iv) administrar los Certificados del Cliente y las Claves de Seguridad o Tokens API correspondientes y cualquier credencial utilizada para la validación del Token API con respecto a la transferencia de archivos de Host a Host/administrados y los canales API, según corresponda; (v) recibir y distribuir materiales, avisos, documentos y correspondencia relacionados con los Procedimientos de Seguridad, según corresponda; y (vi) informar a cada Usuario Autorizado de sus obligaciones en virtud del presente o de la Documentación de Cuenta correspondiente. Los Administradores de Seguridad proporcionarán al Banco, a solicitud del Banco, una lista de Usuarios Autorizados para los canales de Access En Línea y Móvil. En ausencia de una designación válida de un Administrador de Seguridad en cualquier momento, o en el caso de que, después de esfuerzos razonables, el Banco no pueda comunicarse con un Administrador de Seguridad, el Banco puede entregar Dispositivos de Seguridad, Tokens API (y cualquier credencial de asistente) y materiales, y entregar/recibir Claves de seguridad a/de cualquier persona autorizada para actuar en nombre del Cliente con respecto a las Cuentas.

2.9 **Procesamiento.** El Cliente reconoce que la aplicación de los Procedimientos de Seguridad y cualquier control implementado unilateralmente por el Banco puede

2.6. **Confidentiality/Security Breach.** The Customer will be responsible for safeguarding and ensuring that the Security Procedures, Security Devices, API Tokens and any credentials used for the validation of the API Token are known to and used (i) in the case of Access Online and Mobile, only by individuals designated as users by the Security Administrators ("**Authorized Users**"), or, (ii) in the case of the Host-to-Host/managed file transfer and API channels, only by the Security Administrators, as applicable. The Customer shall notify the Bank immediately in the event of any loss, theft or unauthorized use of a Security Procedure, a Security Device, API Token, any credentials used for the validation of the API Token or any other breach of security. The Bank may dishonor or disable any Security Device, API Token, any credentials used for the validation of the API Token or any aspect of the Security Procedures at any time without prior notice and will inform the Customer of the same. In addition, each Customer must implement its own physical and logical security, as well as management controls, that appropriately protect the hardware, software, and access controls used in the transaction process from unauthorized access and use.

2.7. **Security Administrator Designation.** The Customer shall designate Security Administrators who shall have equal authority as specified in Section 2.8 below. The Bank is entitled to rely on any such designation of a Security Administrator. 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 a reasonable opportunity to act upon it.

2.8. **Security Administrator Responsibilities.** Each Security Administrator shall be authorized by the Customer to and be responsible for (i) designating individuals as Authorized Users with respect to the Access Online and Mobile channels; (ii) identifying the functions of the Service that each Authorized User may access; (iii) requesting, creating, controlling, disseminating, and/or canceling user entitlements with respect to the Access Online and Mobile channels; (iv) managing the Customer's Certificates and corresponding Security Keys or API Tokens and any credentials used for the validation of the API Token with respect to the Host-to-Host/managed file transfer and API channels, as applicable; (v) receiving and distributing materials, notices, documents and correspondence relating to the Security Procedures, as applicable; and (vi) advising each Authorized User of his/her obligations hereunder or under any of the applicable Account Documentation. The Security Administrators shall provide to the Bank, upon the Bank's request, a list of Authorized Users for the Access Online and Mobile channels. In the absence of a valid designation of a Security Administrator at any time or in the event that, after reasonable efforts, the Bank is unable to contact a Security Administrator, the Bank may deliver Security Devices, API Tokens (and any attendant credentials) and materials and deliver/receive Security Keys to/from any person authorized to act on behalf of the Customer with respect to the Accounts.

2.9. **Processing.** The Customer acknowledges that the application of the Security Procedures and any controls unilaterally implemented by the Bank may cause delays

causar demoras en el procesamiento de las Instrucciones o provocar que el Banco se niegue a ejecutar una Instrucción.

3. Acceso a la Red Abierta; Equipo

EL SERVICIO SE PROPORCIONA "TAL CUAL ES" Y "SEGÚN ESTÉ DISPONIBLE". AL GRADO MÁXIMO PERMITIDO POR LA LEY APLICABLE, TODAS LAS GARANTÍAS Y REPRESENTACIONES, EXPRESAS, ESTATUTARIAS O IMPLÍCITAS, CON RESPECTO AL SERVICIO, SE EXCLUYEN POR LA PRESENTE, INCLUYENDO CUALQUIER GARANTÍA DE COMERCIABILIDAD, DE CUALIDAD SATISFACTORIA, DE ADECUACIÓN A UN FIN ESPECÍFICO, CURSO DE NEGOCIACIÓN O DE USO DE COMERCIO O GARANTÍAS DE NO INFRACCIÓN O GARANTÍAS CON RESPECTO A CUALQUIER RESULTADO QUE SE OBTENGA DEL USO DEL SERVICIO. EN LA MEDIDA EN QUE CUALQUIER GARANTÍA IMPLÍCITA NO PUEDA SER RENUNCIADA BAJO LA LEY APLICABLE, CUALQUIER GARANTÍA IMPLÍCITA TIENE UNA DURACIÓN LIMITADA A 30 DÍAS A PARTIR DE LA FECHA DE ENTREGA INICIAL DEL SERVICIO RELEVANTE. EL BANCO Y LOS DATOS DE SUS TERCEROS Y LOS PROVEEDORES DE SERVICIOS NO GARANTIZAN LA SEGURIDAD, SECUENCIA, PUNTUALIDAD, PRECISIÓN, RENDIMIENTO O INTEGRIDAD DE LOS DATOS O QUE CUALQUIER PARTE DEL SERVICIO ESTARÁ LIBRE DE ERRORES, SIN RETRASOS O SIN INTERRUPCIONES.

El Cliente es responsable, a su entero cargo, de obtener, instalar, mantener y operar todos los navegadores, software, hardware, equipos de telecomunicaciones u otros equipos (colectivamente, el "**Sistema**") necesarios para que el Cliente acceda y utilice el Servicio de acuerdo con la configuración del sistema recomendada por el Banco. El Banco no respalda ningún Sistema o sitio de terceros, a pesar de que el Banco puede recomendar ciertos Sistemas o proporcionar un enlace a un sitio de terceros donde el Cliente puede descargar software. El Cliente deberá mantener en todo momento un antivirus, anti-spyware u otro software de seguridad actualizado y efectivo y tomará todas las medidas razonables para mantener la seguridad de su Sistema. El Cliente reconoce que existen ciertos riesgos de seguridad, corrupción, error de transmisión y disponibilidad de acceso asociados con el uso de redes abiertas como Internet. El Cliente reconoce además que ha realizado una evaluación independiente de la idoneidad de Internet, el Sistema y los Procedimientos de Seguridad en relación con el uso del Servicio. El Cliente asume todos los riesgos y responsabilidades asociados con la operación, desempeño y seguridad de su Sistema y el uso de Internet u otras redes abiertas, falla o uso del equipo, hardware, navegadores, sistemas operativos y/u otro software del Cliente o de terceros. o programas y servicios o personas fuera del control del Banco, y el Banco se exime de todos esos riesgos. El Cliente no utilizará ningún equipo, hardware, software o programa que dañe al Banco. El Cliente se compromete a indemnizar y mantener al Banco, y a sus agentes, empleados, funcionarios y directores, indemnes de y contra todos y cada uno de los reclamos, daños, demandas, juicios, responsabilidades, pérdidas, costos y gastos que surjan, directa o indirectamente, del uso por parte del Cliente del software o programa del Cliente o de terceros. El Banco puede, a su discreción, brindar capacitación o información sobre las mejores prácticas al Cliente de forma periódica, pero al hacerlo, no será considerado un consultor o asesor con respecto a la ciberseguridad.

4. Instrucciones; Datos

4.1 El Cliente será el único responsable de la autenticidad y precisión, tanto en cuanto al contenido como a la forma, de todas las Instrucciones dadas al Banco en nombre del Cliente y verificadas mediante el Procedimiento de Seguridad correspondiente.

in processing Instructions or result in the Bank declining to execute an Instruction.

3. Open Network Access; Equipment

THE SERVICE IS PROVIDED “AS IS” AND "AS AVAILABLE". TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, ALL WARRANTIES AND REPRESENTATIONS, EXPRESS, STATUTORY OR IMPLIED, WITH REGARD TO THE SERVICE ARE HEREBY DISCLAIMED, INCLUDING ANY WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE AND COURSE OF DEALING OR USAGE OF TRADE OR WARRANTIES OF NON-INFRINGEMENT OR WARRANTIES AS TO ANY RESULTS TO BE OBTAINED FROM THE USE OF THE SERVICE. TO THE EXTENT THAT ANY IMPLIED WARRANTIES CANNOT BE DISCLAIMED UNDER APPLICABLE LAW, ANY SUCH IMPLIED WARRANTIES ARE LIMITED IN DURATION TO 30 DAYS FROM THE INITIAL DELIVERY DATE OF THE RELEVANT SERVICE. THE BANK AND ITS THIRD PARTY DATA AND SERVICE PROVIDERS DO NOT WARRANT OR GUARANTEE THE SECURITY, SEQUENCE, TIMELINESS, ACCURACY, PERFORMANCE OR COMPLETENESS OF THE DATA OR THAT ANY PART OF THE SERVICE WILL BE ERROR-FREE, WITHOUT DELAY OR UNINTERRUPTED.

The Customer is responsible for, at its sole expense, obtaining, installing, maintaining and operating all browsers, software, hardware, telecommunications equipment or other equipment (collectively, “**System**”) necessary for the Customer to access and use the Service in accordance with the Bank’s recommended system configuration. The Bank makes no endorsement of any System or third party site, notwithstanding that the Bank may recommend certain Systems or provide a link to a third party site where the Customer may download software. The Customer shall at all times maintain current and effective anti-virus, anti-spyware or other security software and shall take all reasonable measures to maintain the security of its System. The Customer acknowledges that there are certain security, corruption, transmission error, and access availability risks associated with using open networks such as the Internet. The Customer further acknowledges that it has made an independent assessment of the adequacy of the Internet, the System and the Security Procedures in connection with the use of the Service. The Customer assumes all risks and liabilities associated with the operation, performance and security of its System and the use of the Internet or other open networks, failure or use of Customer’s or third party equipment, hardware, browsers, operating systems and/or other software or programs, and services or persons outside of the Bank’s control, and the Bank disclaims all such risks. The Customer shall not use any equipment, hardware, software or program that harms the Bank. The Customer agrees to indemnify and hold the Bank, and its agents, employees, officers and directors, harmless from and against any and all claims, damages, demands, judgments, liabilities, losses, costs and expenses arising, directly or indirectly, from the Customer’s use of Customer’s or third-party software or program. The Bank may in its discretion provide training or information on best practices to the Customer from time to time but in so doing it will not be considered a consultant or advisor with respect to cybersecurity.

4. Instructions; Data

4.1. The Customer shall be solely responsible for the genuineness and accuracy, both as to content and form, of all Instructions given to the Bank’s in the Customer’s name and verified through the applicable Security Procedure.

4.2 El Cliente reconoce que los Datos pueden no haber sido revisados por el Banco, pueden ser inexactos y pueden actualizarse y ajustarse periódicamente. El Banco no está obligado a garantizar la exactitud de los Datos y no será responsable de ninguna pérdida o daño que surja de la inexactitud de los Datos. Además, el Banco no tendrá ninguna responsabilidad por la recepción o visualización por cualquier parte de los Datos enviados a los destinos designados por el Cliente, incluidos, entre otros, direcciones de correo electrónico, números de fax y teléfono.

5. Garantías del Cliente

El Cliente declara, garantiza y se compromete al Banco que: (i) antes de enviar cualquier documento o Instrucción que designe Usuarios Autorizados, el Cliente deberá obtener de cada individuo mencionado en dicho documento o Instrucción todos los consentimientos necesarios para que el Banco pueda procesar los datos allí establecidos con el fin de proporcionar el Servicio; (ii) el Cliente ha designado con precisión por escrito o electrónicamente la ubicación geográfica de sus Usuarios Autorizados y proporcionará todas las actualizaciones de dicha información; (iii) el Cliente no accederá al Servicio desde ninguna jurisdicción que el Banco le informe o cuando el Cliente tenga conocimiento de que el Servicio no está autorizado; y (iv) los Procedimientos de Seguridad ofrecidos al Cliente se ajustan a los deseos y necesidades del Cliente y el Cliente no ha solicitado Procedimientos de Seguridad distintos de los acordados expresamente por el Cliente y el Banco. Por la presente, el Cliente declara, garantiza y se compromete al Banco que estos Términos de Servicio constituyen sus obligaciones legales y vinculantes aplicables de acuerdo con sus términos.

6. Disposiciones Varias

6.1 Las disposiciones específicas de jurisdicción adicional establecidas en el Anexo son aplicables al Cliente en función del domicilio del Cliente. Cuando se apliquen leyes o reglamentos locales de cualquier jurisdicción como resultado de que los Usuarios Autorizados del Cliente accedan al Servicio desde dicha jurisdicción o como resultado de la ubicación de dichas cuentas en dicha jurisdicción, las disposiciones jurisdiccionales específicas de esa jurisdicción se establecen en el Anexo adjunto se aplicarán al uso del Servicio por parte de dichos Usuarios Autorizados.

6.2 Los presentes Términos de Servicio se regirán e interpretarán de acuerdo con las leyes del Estado de Nueva York, EE.UU. (sin referencia al conflicto de leyes y reglas de los mismos).

6.3 Todas las disputas relacionadas con los presentes Términos de Servicio que surjan únicamente fuera de los Estados Unidos serán finalmente resueltas bajo las Reglas de Arbitraje de la Cámara de Comercio Internacional por uno o más árbitros designados de acuerdo con dichas Reglas. El lugar del arbitraje será (i) Singapur, donde la disputa surge únicamente en Asia y (ii) Londres, donde la disputa surge en otro lugar (que no sea Estados Unidos) y el arbitraje se llevará a cabo en inglés, excepto en el caso de (a) disputas únicamente entre un Cliente domiciliado en la República Popular de China y JPMorgan Chase Bank (China) Company Limited, las cuales se someterán a la Comisión de Arbitraje Comercial y Económico Internacional de China ("**CIETAC**") para su arbitraje de conformidad con sus reglas vigentes en el momento en que la solicitud se realiza, siendo el lugar del arbitraje Beijing y el arbitraje en inglés; y (b) las disputas que involucren a un Cliente domiciliado en Taiwán se someterán irrevocablemente a la jurisdicción exclusiva de los tribunales del Estado de Nueva York y del Tribunal de Distrito de los Estados Unidos ubicado en el distrito de Manhattan, en la Ciudad

4.2. The Customer acknowledges that Data may not have been reviewed by the Bank, may be inaccurate, and may be periodically updated and adjusted. The Bank is not obligated to assure the accuracy of Data and will not be liable for any loss or damage arising out of the inaccuracy of Data. 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).

5. Customer Warranties

The Customer represents, warrants and covenants to the Bank that: (i) prior to submitting any document or Instruction that designates Authorized Users, the Customer shall obtain from each individual referred to in such document or Instruction all necessary consents to enable the Bank to process the data set out therein for the purposes of providing the Service; (ii) the Customer has accurately designated in writing or electronically the geographic location of its Authorized Users and shall provide all updates to such information; (iii) the Customer shall not access the Service from any jurisdiction which the Bank informs the Customer or where the Customer has knowledge that the Service is not authorized; and (iv) the Security Procedures offered to the Customer conform to the Customer's wishes and needs and the Customer has not requested Security Procedures other than those expressly agreed by the Customer and the Bank. The Customer hereby represents, warrants and covenants to the Bank that these Service Terms constitute its legal and binding obligations enforceable in accordance with its terms.

6. Miscellaneous

6.1. The additional jurisdiction specific provisions set forth in the attached Exhibit are applicable to the Customer based on the domicile of the Customer. Where any local laws or regulations of any jurisdiction apply as a result of the Customer's Authorized Users accessing the Service from such jurisdiction or as a result of the location of such accounts in such jurisdiction, the jurisdictional specific provisions of that jurisdiction set forth in the attached Exhibit shall apply to the use of the Service by such Authorized Users.

6.2. These Service Terms shall be governed by and construed in accordance with the laws of the State of New York, USA (without reference to the conflict of laws rules thereof).

6.3. All disputes relating to or in connection with these Service Terms solely arising outside the United States shall be finally settled under the Rules of Arbitration of the International Chamber of Commerce by one or more arbitrators appointed in accordance with the said Rules. The place of arbitration shall be (i) Singapore where the dispute arises solely in Asia and (ii) London where the dispute arises elsewhere (other than the United States) and the arbitration shall be conducted in English, except that (a) disputes solely between a Customer domiciled in the People's Republic of China and JPMorgan Chase Bank (China) Company Limited shall be submitted to the China International Economic and Trade Arbitration Commission ("**CIETAC**") for arbitration in accordance with its rules in effect at the time an application is made, with the place of arbitration being Beijing and the arbitration being conducted in English; and (b) disputes involving a Customer domiciled in Taiwan shall be irrevocably submitted to the exclusive jurisdiction of the courts of the State of New York and the United States District Court located in the borough of Manhattan in New York City. With respect to any dispute, suit, action or proceedings arising in the United States relating to these Service Terms, the Customer irrevocably submits to the exclusive

de Nueva York. Con respecto a cualquier disputa, demanda, acción o procedimiento que surja en los Estados Unidos en relación con los presentes Términos de Servicio, el Cliente se someterá irrevocablemente a la jurisdicción exclusiva de los tribunales del Estado de Nueva York y el Tribunal de Distrito de los Estados Unidos, ubicado en el distrito de Manhattan, Ciudad de Nueva York.

7. Móvil

7.1 La aceptación del uso del servicio del Banco de notificaciones mediante mensajes SMS y/o del canal Access Móvil constituye la autorización del Cliente para que el Banco envíe Datos, notificaciones de mensajes y alertas a través de cualquier proveedor de servicios de comunicación, incluidos los proveedores de Internet y telecomunicaciones, los cuales se considerarán como actuando en calidad de agentes del Cliente. Dichos proveedores no podrán encriptar las comunicaciones.

7.2 Es posible que se solicite a los Usuarios Autorizados que acepten un acuerdo de aplicación o una licencia para descargar Access Móvil. El Cliente reconoce que la Documentación de la Cuenta en todos los casos regirá la prestación de estos servicios.

7.3 El Cliente reconoce que el Banco no será responsable por retrasos en los Datos, notificaciones de mensajes o alertas enviadas a través de cualquier dispositivo móvil.

jurisdiction of the courts of the State of New York and the United States District Court located in the borough of Manhattan in New York City.

7. Mobile

7.1. Accepting use of the Bank's SMS text notification service and/or Access Mobile channel constitutes the Customer's authorization for the Bank to send 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.

7.2. Authorized Users may be required to accept an application agreement or license in order to download Access Mobile. The Customer acknowledges that the Account Documentation shall in all cases govern the provision of these services.

7.3. The Customer acknowledges that the Bank shall not be liable for any delays in any Data, message notification or alert delivered via any mobile device.