J.P. MORGAN TREASURY SERVICES ELECTRONIC CHANNELS SERVICE TERMS (ENGLISH AND VIETNAMESE) CÁC ĐIỀU KHOẢN DỊCH VỤ KÊNH ĐIỆN TỬ DỊCH VỤ QUỸ CỦA J.P. MORGAN (ENGLISH AND VIETNAMESE)

V1.4_11_23_20

1. Service and Service Terms. Dịch Vụ và các Điều Khoản Dịch Vụ

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.

Ngân Hàng cung cấp dịch vụ ("**Dịch Vụ**") để truy cập bằng phương tiện điện tử vào thông tin tài khoản, các báo cáo và dữ liệu của Khách Hàng (gọi chung là "**Dữ Liệu**") và để truyền tải bằng phương tiện điện tử đến cho Ngân Hàng các thông điệp, yêu cầu cung cấp dịch vụ, và các chỉ thị thanh toán và không thanh toán (trong mỗi trường hợp được gọi là "**Chỉ Thị**") và từ Ngân Hàng các thông điệp, thông báo và cảnh báo, thông qua các kênh J.P. Morgan Access® Online℠, J.P. Morgan Access® Mobile℠, J.P. Morgan chuyển tập tin quản lý/máy chủ-đến-máy chủ và J.P. Morgan Treasury Services API. Ngân Hàng bảo lưu quyền điều chỉnh các ứng dụng và các sản phẩm được dành sẵn thông qua Dịch Vụ. Dịch Vụ được điều chỉnh bởi các điều khoản này ("**các Điều Khoản Dịch Vụ**"), mà có bao gồm các điều khoản của Ngân Hàng điều chỉnh các dịch vụ và tài khoản kinh doanh, bao gồm cả các điều khoản dịch vụ điều chỉnh việc Ngân Hàng xử lý các Chỉ Thị được truyền tải thông qua Dịch Vụ (gọi chung là "**Tài Liệu Tài Khoản**"), như có thể được sửa đổi trong từng thời điểm. Nếu và trong chừng mực có mâu thuẫn giữaTài Liệu Tài Khoản và các Điều Khoản Dịch Vụ này, thì các quy định của các Điều Khoản Dịch Vụ này sẽ được ưu tiên áp dụng. Các thuật ngữ viết hoa được sử dụng trong các Điều Khoản Dịch Vụ này và không được định nghĩa khác đi sẽ có ý nghĩa như được quy định trong các Điều Khoản Tài Khoản Toàn Cầu hoặc các điều khoản tài khoản khác được áp dụng cho Khách Hàng. JPMorgan Chase Bank, N.A. được thành lập theo pháp luật Hoa Kỳ và là một công ty trách nhiệm hữu hạn.

2. Security Procedures and Other Controls Thủ Tục Bảo Mật và các Biện Pháp Kiểm Soát Khác

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.

Quy định chung. Các thủ tục bảo mật dành cho mỗi kênh được quy định dưới đây, như có thể được sửa đổi bằng thông báo gửi đến Khách Hàng thông qua bất kỳ phương tiện nào (được gọi riêng là "**Thủ Tục Bảo Mật**"). Bất kỳ Chỉ Thị nào đã được xác thực thông qua một Thủ Tục Bảo Mật sẽ có hiệu lực như là Chỉ Thị của Khách Hàng, dù có được cho phép hay không, và dù Chỉ Thị đó có thể làm phát sinh thấu chi đối với một Tài Khoản. Các biện pháp kiểm soát do Ngân Hàng đơn phương thực hiện sẽ không được xem là Thủ Tục Bảo Mật cho mục đích của các Điều Khoản này trừ khi được xác định rõ ràng bằng văn bản là Thủ Tục Bảo Mật. Khách Hàng chịu trách nhiệm thực hiện bất kỳ thủ tục và yêu cầu nào nêu trong các tài liệu có liên quan do Ngân Hàng cung cấp cho Khách Hàng, cũng như bất kỳ sửa đổi nào về sau đối với các thủ tục và yêu cầu được xác lập để tăng cường các Thủ Tục Bảo Mật.

2.2. Security Procedures and Other Controls for Access Online and Mobile Channels. Thủ Tục Bảo Mật và các Biện Pháp Kiểm Soát Khác cho các Kênh Truy Cập Trực Tuyến và Di Động

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), a token code generated by a Bank issued or approved security device ("**Security Device**") assigned to that Authorized User and Bank transaction review as specified in Section 2.5.

Truy Cập Trực Tuyến. Thủ Tục Bảo Mật để xác minh các Chỉ Thị thanh toán được đưa ra dưới tên của Khách Hàng thông qua kênh Truy Cập Trực Tuyến là xác nhận ID người sử dụng và mật khẩu bảo mật của một Người Sử Dụng Được Phép (như được định nghĩa tại Phần 2.6 dưới đây), một mã token được tạo ra bởi một thiết bị bảo mật do Ngân Hàng phát hành hoặc chấp thuận ("**Thiết Bị Bảo Mật**") được cấp phát cho Người Sử Dụng Được Phép đó và việc rà soát giao dịch của Ngân Hàng như được nêu cụ thể tại Phần 2.5.

2.2.2. **Access Mobile.** The Security Procedure for verifying payment Instructions given in the Customer's name via the Access Mobile channel is either (i) validation of the registration with the Bank of the mobile device, a biometric identifier, and the private swipe key of an Authorized User (as defined in Section 2.6 below) and transaction review as specified in Section 2.5 or (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 Security Device assigned to that Authorized User and transaction review as specified in Section 2.5.

Truy Cập Di Động. Thủ Tục Bảo Mật để xác minh các Chỉ Thị thanh toán được đưa ra dưới tên của Khách Hàng thông qua kênh Truy Cập Di Động là (i) xác nhận việc đăng ký với Ngân Hàng thiết bị di động, một thiết bị nhận diện sinh trắc học và khóa quét riêng của Người Sử Dụng Được Phép (như được định nghĩa tại Phần 2.6 dưới đây) và việc rà soát giao dịch như được nêu cụ

thể tại Phần 2.5 hoặc (ii) xác nhận ID người sử dụng và mật khẩu bảo mật của một Người Sử Dụng Được Phép (như được định nghĩa tại Phần 2.6 dưới đây), một mã token được tạo ra bởi một Thiết Bị Bảo Mật được cấp phát cho Người Sử Dụng Được Phép đó và việc rà soát giao dịch như được nêu cụ thể tại Phần 2.5.

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.

Các Biện Pháp Kiểm Soát dành cho Khách Hàng. Đối với Truy Cập Trực Tuyến và Di Động, Khách Hàng có thể lựa chọn áp dụng các biện pháp kiểm soát nhất định do Ngân Hàng cung cấp cho Khách Hàng trong từng thời điểm được đề ra nhằm giảm rủi ro giao dịch trái phép cho Khách Hàng. Khách Hàng chịu trách nhiệm lựa chọn biện pháp kiểm soát nào phù hợp cho mình có tính đến, ngoài những điều khác, tính chất và quy mô công việc kinh doanh của Khách Hàng, bao gồm cả quy mô, loại và tần suất của các lệnh thanh toán thường được đưa ra cho Ngân Hàng, và tính chất của môi trường kỹ thuật, các biện pháp kiểm soát kế toán nội bộ và các thủ tục và chính sách bảo mật thông tin của Khách Hàng (gọi chung là "**các Biện Pháp Kiểm Soát Nội Bộ Của Khách Hàng**"). Thủ Tục Bảo Mật được xác lập theo thỏa thuận của Khách Hàng và Ngân Hàng trong các Điều Khoản này được xác lập có xét đến các Biện Pháp Kiểm Soát Nội Bộ Của Khách Hàng do Khách Hàng áp dụng. Để tránh nhầm lẫn, không có biện pháp kiểm soát nào nêu tại Phần này là một phần trong Thủ Tục Bảo Mật cho các kênh.

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**".

Thủ Tục Bảo Mật và thủ tục chứng thực cho kênh chuyển tập tin quản lý/máy chủ-đến-máy chủ. Thủ Tục Bảo Mật để xác minh các Chỉ Thị thanh toán được đưa ra dưới tên của Khách Hàng thông qua kênh chuyển tập tin quản lý/máy chủ-đến-máy chủ là chứng thực chữ ký số, để xác thực các tập tin được chuyển trên cơ sở khóa bảo mật tương ứng ("**Chứng Thực Chữ Ký**") và việc rà soát giao dịch như được nêu cụ thể tại Phần 2.5. Khách Hàng và Ngân Hàng sẽ áp dụng các thủ tục sau đây cho việc sử dụng chứng thực truyền tải, để thiết lập phiên bảo mật giữa Ngân Hàng và Khách Hàng trên cơ sở khóa bảo mật tương ứng ("**Chứng Thực Truyền Tải**") và Chứng Thực Chữ Ký. Chứng Thực Chữ Ký và Chứng Thực Truyền Tải được gọi riêng trong đây là "**Chứng Thực**" và khóa bảo mật tương ứng được gọi là "**Khóa Bảo Mật**".

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 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.

Yêu cầu và thủ tục Chứng Thực. Khách Hàng tuân thủ các thủ tục và yêu cầu của Ngân Hàng đối với Chứng Thực và Khóa Bảo Mật được thông báo cho Khách Hàng, bao gồm nhưng không chỉ giới hạn ở thời hạn hiệu lực của Chứng Thực, thông số mật mã học và độ an toàn của khóa, như được sửa đổi trong từng thời điểm. Bất kỳ yêu cầu nào với Ngân Hàng để bổ sung, cập nhật hoặc xóa Khóa Bảo Mật phải bao gồm cả Chứng Thực áp dụng, một tập tin văn bản hoặc cam đoan cụ thể khác về Khóa Bảo Mật chung của Chứng Thực đó và bất kỳ thông tin nào khác theo cách thức và dưới hình thức do Ngân Hàng chỉ định. Ngân Hàng có quyền dựa vào bất kỳ yêu cầu nào mà Ngân Hàng một cách trung thực cho rằng đã được gửi bởi quản trị viên bảo mật được chỉ định ("**Quản Trị Viên Bảo Mật** "), bất kể Quản Trị Viên Bảo Mật nêu trên có thể là bên thứ ba hành động thay mặt cho Khách Hàng.

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.

Hết hạn Chứng Thực. Bất kể bất kỳ thông báo nhắc nhở nào Ngân Hàng có thể gửi cho Khách Hàng về việc Chứng Thực của Khách Hàng sắp hết hạn, Khách Hàng xác nhận rằng Khách Hàng hoàn toàn chịu trách nhiệm cập nhật Chứng Thực trước ngày Chứng Thực hết hạn. Ngân Hàng không chịu bất kỳ trách nhiệm nào về bất kỳ tổn thất hoặc thiệt hại nào (bao gồm cả, để tránh nhầm lẫn, bất kỳ tổn thất hoặc thiệt hại gián tiếp, đặc biệt, mang tính chất trừng phạt hoặc hậu quả) phát sinh từ việc Khách Hàng không cập nhật Chứng Thực của mình một cách kịp thời. Để cho phép thực hiện đúng các thủ tục hành chính, và tránh gián đoạn bất kỳ dịch vụ hoặc thủ tục khẩn cấp nào, Khách Hàng phải yêu cầu thay đổi Chứng Thực ít nhất 30 ngày trước ngày hết hạn Chứng Thực trên thực tế.

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.

Thủ Tục Bảo Mật và thủ tục Chứng Thực/ token đối với kênh API. Thủ Tục Bảo Mật để xác minh các Chỉ Thị thanh toán được đưa ra dưới tên của Khách Hàng thông qua kênh API là xác minh Chứng Thực Chữ Ký và rà soát giao dịch như được nêu tại Phần 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**").

Phiên bảo mật. Khách Hàng và Ngân Hàng sẽ xác lập phiên bảo mật giữa Khách Hàng và Ngân Hàng bằng cách xác nhận (i) Chứng Thực Truyền Tải hoặc (ii) token do Ngân Hàng tạo ra ("**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.

Yêu cầu và thủ tục Chứng Thực. Khách Hàng và Ngân Hàng sẽ áp dụng các thủ tục nêu tại Phần 2.3.1 và 2.3.2 cho việc sử dụng các Chứng Thực đối với kênh API.

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.

Yêu cầu và thủ tục API Token. Khách Hàng phải tuân thủ các yêu cầu và thủ tục của Ngân Hàng đối với API Token, như được sửa đổi trong từng thời điểm, bao gồm nhưng không chỉ giới hạn ở việc tạo và bảo vệ an toàn bất kỳ thông tin đăng nhập nào được sử dụng để xác nhận API Token được thông báo cho Khách Hàng. Ngân Hàng có quyền hủy bỏ API Token vào bất kỳ thời điểm nào, bao gồm cả việc dựa vào yêu cầu hoặc thông tin liên lạc liên quan đến API Token mà Ngân Hàng một cách trung thực cho là đã được gửi bởi Quản Trị Viên Bảo Mật, bất kể là Quản Trị Viên Bảo Mật đó có thể là bên thứ ba hành động thay mặt cho Khách Hàng. Bất kỳ yêu cầu nào với Ngân Hàng về việc cập nhật API Token sẽ phải được thực hiện hoàn toàn theo cách thức và dưới hình thức do Ngân Hàng chỉ định.

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.

Rà soát giao dịch. Bên cạnh các Thủ Tục Bảo Mật được mô tả ở trên, Thủ Tục Bảo Mật áp dụng cho từng kênh cũng bao gồm việc rà soát giao dịch dựa trên một số đặc điểm rủi ro. Việc rà soát giao dịch sẽ được thực hiện theo các giao thức hợp lý về mặt thương mại do Ngân Hàng lựa chọn. Khách Hàng có thể được yêu cầu xác thực bổ sung, chẳng hạn như gọi điện thoại lại để xác minh, để hoàn tất một số giao dịch do Ngân Hàng xác định thông qua việc rà soát giao dịch.

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.

Vi phạm bảo mật/an ninh. Khách Hàng chịu trách nhiệm bảo vệ an toàn và bảo đảm rằng các Thủ Tục Bảo Mật, Thiết Bị Bảo Mật, API Token và bất kỳ thông tin đăng nhập nào được sử dụng để xác nhận API Token được biết đến và được sử dụng (i) trong trường hợp Truy Cập Trực Tuyến và Di Động, chỉ bởi những cá nhân được Quản Trị Viên Bảo Mật chỉ định là người sử dụng ("**Người Sử Dụng Được Phép**"), hoặc, (ii) trong trường hợp các kênh chuyển tập tin quản lý/máy chủ-đến-máy chủ và API, chỉ bởi Quản Trị Viên Bảo Mật, như có liên quan. Khách Hàng phải thông báo ngay cho Ngân Hàng trong trường hợp có bất kỳ tổn thất, trộm cắp hoặc việc sử dụng trái phép nào đối với Thủ Tục Bảo Mật, Thiết Bị Bảo Mật, API Token, bất kỳ thông tin đăng nhập nào được sử dụng cho việc xác nhận API Token hoặc bất kỳ trường hợp vi phạm an ninh nào khác. Ngân Hàng có thể từ chối chấp nhận hoặc vô hiệu hóa bất kỳ Thiết Bị Bảo Mật, API Token, bất kỳ thông tin đăng nhập nào được sử dụng để xác nhận API Token hoặc bất kỳ phương diện nào của Thủ Tục Bảo Mật vào bất kỳ thời điểm nào mà không cần thông báo trước và sẽ thông báo cho Khách Hàng về việc từ chối chấp nhận hoặc vô hiệu hóa trên. Ngoài ra, mỗi Khách Hàng phải thực hiện các biện pháp kiểm soát an ninh vật lý và lo-gic, cũng như các biện pháp kiểm soát quản lý của riêng mình mà bảo vệ một cách thích hợp các phần cứng, phần mềm và các biện pháp kiểm soát truy cập được sử dụng trong quá trình giao dịch khỏi bị truy cập và sử dụng trái phép.

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.

Chỉ định Quản Trị Viên Bảo Mật. Khách Hàng chỉ định các Quản Trị Viên Bảo Mật, là những người có thẩm quyền ngang nhau như được nêu tại Phần 2.8 dưới đây. Ngân Hàng được quyền dựa vào bất kỳ việc chỉ định Quản Trị Viên Bảo Mật nào nêu trên. Khách Hàng đồng ý thông báo cho Ngân Hàng về bất kỳ thay đổi nào đối với các Quản Trị Viên Bảo Mật theo cách thức và hình thức mà Ngân Hàng chỉ định. Bất kỳ thay đổi nào nêu trên sẽ có hiệu lực tại thời điểm Ngân Hàng đã nhận được thông báo đó và đã có cơ hội hợp lý để hành động theo thông báo.

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.

Trách nhiệm Của Quản Trị Viên Bảo Mật. Mỗi Quản Trị Viên Bảo Mật sẽ được Khách Hàng ủy quyền để và chịu trách nhiệm về việc (i) chỉ định cá nhân nào là Người Sử Dụng Được Phép đối với các kênh Truy Cập Trực Tuyến và Di Động; (ii) xác định các chức năng của Dịch Vụ mà Người Sử Dụng Được Phép có thể truy cập; (iii) đề nghị, tạo lập, kiểm soát, phổ biến, và/hoặc chấm dứt các quyền của người sử dụng đối với các kênh Truy Cập Trực Tuyến và Di Động; (iv) quản lý các Chứng Thực của Khách Hàng và Khóa Bảo Mật hoặc API Token tương ứng và bất kỳ thông tin đăng nhập nào được sử dụng để xác nhận API Token đối với các kênh chuyển tập tin quản lý/máy chủ-đến-máy chủ và API, như có liên quan; (v) nhận và phân phát các tài liệu, thông báo, văn bản và thư từ liên quan đến các Thủ Tục Bảo Mật, như có liên quan; và (v) thông báo cho từng Người Sử Dụng Được Phép về các nghĩa vụ của họ theo các Điều Khoản này hoặc theo bất kỳ Tài Liệu Tài Khoản nào được áp dụng. Các Quản Trị Viên Bảo Mật cung cấp cho Ngân Hàng, khi Ngân Hàng có yêu cầu, danh sách những Người Sử Dụng Được Phép cho các kênh Truy Cập Trực Tuyến và Di Động . Nếu vào bất kỳ lúc nào không có Quản Trị Viên Bảo Mật được chỉ định hợp lệ hoặc trong trường hợp sau khi đã nỗ lực hợp lý mà Ngân Hàng vẫn không thể liên hệ với Quản Trị Viên Bảo Mật, thì Ngân Hàng có thể giao các Thiết Bị Bảo Mật, API Token (và bất kỳ thông tin đăng nhập kèm theo nào) và các tài liệu và giao/nhận Khóa Bảo Mật cho/từ bất kỳ người nào được phép hành động thay mặt cho Khách Hàng liên quan đến các Tài Khoản.

2.9. Processing. The Customer acknowledges that the application of the Security Procedures and any controls unilaterally implemented by the Bank may cause delays in processing Instructions or result in the Bank declining to execute an Instruction.

Xử lý. Khách Hàng xác nhận rằng việc áp dụng các Thủ Tục Bảo Mật và bất kỳ biện pháp kiểm soát nào do Ngân Hàng đơn phương thực hiện có thể làm chậm trễ việc xử lý các Chỉ Thị hoặc dẫn đến việc Ngân Hàng từ chối thực hiện một Chỉ Thị.

3. Open Network Access; Equipment
Truy cập mạng mở; Thiết bị

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.

DỊCH VỤ ĐƯỢC CUNG CẤP TRÊN CƠ SỞ "NHƯ HIỆN CÓ" VÀ "NHƯ CÓ SẴN". TRONG CHỪNG MỰC TỐI ĐA ĐƯỢC PHÁP LUẬT ÁP DỤNG CHO PHÉP, TẤT CẢ CÁC TUYÊN BỐ VÀ BẢO ĐẢM, CHO DÙ LÀ RÕ RÀNG, THEO LUẬT ĐỊNH HOẶC NGẦM ĐỊNH, ĐỐI VỚI DỊCH VỤ THÔNG QUA ĐÂY ĐƯỢC KHƯỚC TỪ TRÁCH NHIỆM, BAO GỒM CẢ BẤT KỲ BẢO ĐẢM NÀO VỀ SỰ PHÙ HỢP CHO CÁC MỤC ĐÍCH CHUNG, CHẤT LƯỢNG THỎA ĐÁNG, TÍNH THÍCH HỢP CHO CÁC MỤC ĐÍCH CỤ THỂ VÀ PHƯƠNG THỨC TIẾN HÀNH GIAO DỊCH HOẶC TẬP QUÁN THƯƠNG MẠI HOẶC CÁC BẢO ĐẢM VỀ KHÔNG XÂM PHẠM HOẶC BẢO ĐẢM VỀ BẤT KỲ KẾT QUẢ NÀO CÓ ĐƯỢC TỪ VIỆC SỬ DỤNG DỊCH VỤ. TRONG CHỪNG MỰC BẤT KỲ BẢO ĐẢM NGẦM ĐỊNH NÀO KHÔNG THỂ ĐƯỢC KHƯỚC TỪ THEO BẤT KỲ PHÁP LUẬT ĐƯỢC ÁP DỤNG NÀO, BẤT KỲ BẢO ĐẢM NGẦM ĐỊNH NÀO NHƯ VẬY ĐƯỢC GIỚI HẠN VỀ THỜI GIAN TRONG VÒNG 30 NGÀY KỂ TỪ NGÀY BAN ĐẦU CUNG CẤP DỊCH VỤ CÓ LIÊN QUAN. NGÂN HÀNG VÀ CÁC NHÀ CUNG CẤP DỊCH VỤ VÀ DỮ LIỆU BÊN THỨ BA CỦA NGÂN HÀNG KHÔNG BẢO ĐẢM HOẶC CAM KẾT VỀ TÍNH BẢO MẬT, TRÌNH TỰ, TÍNH KỊP THỜI, TÍNH CHÍNH XÁC, HIỆU SUẤT HOẶC SỰ ĐẦY ĐỦ CỦA DỮ LIỆU HOẶC RẰNG BẤT KỲ PHẦN NÀO CỦA DỊCH VỤ ĐỀU SẼ KHÔNG CÓ LỖI, KHÔNG BỊ CHẬM TRỄ HOẶC KHÔNG BỊ GIÁN ĐOẠN.

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.

Bằng chi phí hoàn toàn của Khách Hàng, Khách Hàng chịu trách nhiệm về việc có được, cài đặt, duy trì và vận hành tất cả các trình duyệt, phần mềm, phần cứng, thiết bị viễn thông hoặc các thiết bị khác (gọi chung là "**Hệ Thống**") cần thiết để Khách Hàng truy cập và sử dụng Dịch Vụ theo cấu hình hệ thống được Ngân Hàng khuyến nghị. Ngân Hàng không xác nhận bất kỳ Hệ Thống hoặc trang web của bên thứ ba nào, dù Ngân Hàng có thể đề xuất một số Hệ Thống nhất định hoặc cung cấp đường dẫn đến trang web của bên thứ ba nơi Khách Hàng có thể tải xuống phần mềm. Khách Hàng phải luôn duy trì phần mềm diệt vi rút và diệt phần mềm gián điệp hoặc phần mềm bảo mật khác mới nhất và hiệu quả và phải thực hiện tất cả các biện pháp hợp lý để duy trì bảo mật đối với Hệ Thống của mình. Khách Hàng xác nhận rằng có những rủi ro nhất định về bảo mật, hư hại, lỗi truyền tải và khả năng truy cập đi kèm với việc sử dụng các mạng mở như Internet. Khách Hàng xác nhận thêm rằng Khách Hàng đã thực hiện đánh giá độc lập về sự đầy đủ của mạng Internet, Hệ Thống và các Thủ Tục Bảo Mật liên quan đến việc sử dụng Dịch Vụ. Khách Hàng chịu mọi rủi ro và trách nhiệm liên quan đến việc vận hành, hiệu suất và tính bảo mật

của Hệ Thống của mình và việc sử dụng mạng Internet hoặc các mạng mở khác, việc hỏng hóc hoặc việc sử dụng thiết bị, phần cứng, trình duyệt, hệ điều hành và/hoặc các phần mềm hoặc chương trình khác của Khách Hàng hoặc bên thứ ba, và các dịch vụ hoặc những người nằm ngoài sự kiểm soát của Ngân Hàng, và Ngân Hàng không chịu trách nhiệm đối với tất cả các rủi ro đó. Khách Hàng không được sử dụng bất kỳ thiết bị, phần cứng, phần mềm hoặc chương trình nào có thể gây hại cho Ngân Hàng. Khách Hàng đồng ý bồi hoàn và giữ vô hại cho Ngân Hàng, và các đại diện, người lao động, viên chức và giám đốc của Ngân Hàng đối với và liên quan đến bất kỳ và toàn bộ các yêu cầu, tiền bồi thường thiệt hại, đòi hỏi, phán quyết, trách nhiệm, tổn thất, chi phí và phí tổn phát sinh trực tiếp hoặc gián tiếp từ việc Khách Hàng sử dụng phần mềm hoặc chương trình của Khách Hàng hoặc bên thứ ba. Ngân Hàng theo toàn quyền quyết định của mình có thể trong từng thời điểm cung cấp đào tạo hoặc thông tin về các cách thực hành tốt nhất cho Khách Hàng nhưng khi làm như vậy Ngân Hàng sẽ không được xem là bên tư vấn hoặc cố vấn về an ninh mạng.

4. Instructions; Data
Chỉ thị; Dữ liệu

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.

Khách Hàng chịu trách nhiệm hoàn toàn về sự chính xác và trung thực của cả nội dung cũng như hình thức của toàn bộ các Chỉ Thị được đưa ra cho Ngân Hàng dưới tên của Khách Hàng và được xác minh thông qua Thủ Tục Bảo Mật được áp dụng.

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).

Khách Hàng xác nhận rằng Dữ Liệu có thể không được xem xét bởi Ngân Hàng, và có thể không chính xác và có thể được cập nhật và điều chỉnh định kỳ. Ngân Hàng không có nghĩa vụ bảo đảm về sự chính xác của Dữ Liệu và không chịu trách nhiệm về bất kỳ tổn thất hoặc thiệt hại nào phát sinh từ sự không chính xác của Dữ Liệu. Ngoài ra, Ngân Hàng không chịu bất kỳ trách nhiệm nào về việc bất kỳ bên nào nhận hoặc xem Dữ Liệu được gửi đến các nơi được Khách Hàng chỉ định, bao gồm nhưng không chỉ giới hạn ở các địa chỉ email, (các) số điện thoại và số fax.

5. Customer Warranties
Bảo đảm của Khách Hàng

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.

Khách Hàng cam kết, cam đoan và bảo đảm với Ngân Hàng rằng: (i) trước khi nộp bất kỳ văn bản hoặc Chỉ Thị nào chỉ định Người Sử Sụng Được Phép, Khách Hàng phải có được từ mỗi cá nhân được nêu trong văn bản hoặc Chỉ Thị đó mọi sự đồng ý cần thiết để cho phép Ngân Hàng có thể xử lý dữ liệu được nêu trong văn bản đó cho mục đích cung cấp Dịch Vụ; (ii) Khách Hàng đã chỉ định một cách chính xác bằng văn bản hoặc bằng phương tiện điện tử địa điểm địa lý của Người Sử Dụng Được Phép của mình và sẽ cập nhật đầy đủ các thông tin đó; (iii) Khách Hàng không được truy cập Dịch Vụ từ bất kỳ vùng lãnh thổ có thẩm quyền tài phán nào mà Ngân Hàng thông báo cho Khách Hàng hoặc tại đó Khách Hàng biết rằng Dịch Vụ không được cho phép; và (iv) Thủ Tục Bảo Mật được cung cấp cho Khách Hàng phù hợp với mong muốn và nhu cầu của Khách Hàng và Khách Hàng đã không yêu cầu bất kỳ Thủ Tục Bảo Mật nào ngoài những Thủ Tục Bảo Mật được thỏa thuận rõ ràng giữa Khách Hàng và Ngân Hàng. Khách Hàng thông qua đây cam kết, cam đoan và bảo đảm với Ngân Hàng rằng các Điều Khoản Dịch Vụ này cấu thành nghĩa vụ pháp lý mang tính ràng buộc của Khách Hàng mà có thể thi hành theo các quy định của các Điều Khoản Dịch Vụ này.

6. Miscellaneous
Các quy định khác

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.

Các quy định cụ thể bổ sung dành cho vùng lãnh thổ có thẩm quyền tài phán được quy định trong Phụ Lục đính kèm được áp dụng cho Khách Hàng trên cơ sở nơi cư trú của Khách Hàng. Trong trường hợp bất kỳ luật hoặc quy định sở tại của bất kỳ vùng lãnh thổ có thẩm quyền tài phán nào được áp dụng do các Người Sử Dụng Được Phép của Khách Hàng truy cập Dịch Vụ từ vùng lãnh thổ đó hoặc do các tài khoản nêu trên được đặt tại vùng lãnh thổ trên, các quy định cụ thể dành cho vùng lãnh thổ có thẩm quyền tài phán đó nêu tại Phụ Lục đính kèm sẽ được áp dụng cho việc sử dụng Dịch Vụ của các Người Sử Dụng Được Phép nêu trên.

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).

Các Điều Khoản Dịch Vụ này được điều chỉnh bởi và được giải thích theo pháp luật Bang New York, USA (không áp dụng các quy định về xung đột pháp luật của Bang này).

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 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.

Tất cả các tranh chấp liên quan đến hoặc đối với các Điều Khoản Dịch Vụ này phát sinh hoàn toàn bên ngoài Hợp Chủng Quốc Hoa Kỳ sẽ được giải quyết chung thẩm theo các Quy Tắc Trọng Tài của Phòng Thương Mại Quốc Tế bởi một hoặc nhiều trọng tài viên được chỉ định theo các Quy Tắc đó. Địa điểm phân xử trọng tài sẽ là (i) Singapore trong trường hợp tranh chấp phát sinh hoàn toàn tại Châu Á và (ii) Luân Đôn trong trường hợp tranh chấp phát sinh tại nơi khác (ngoại trừ Hợp Chủng Quốc Hoa Kỳ) và việc phân xử trọng tài sẽ được tiến hành bằng tiếng Anh, ngoại trừ là (a) tranh chấp phát sinh hoàn toàn giữa Khách Hàng cư trú tại Cộng Hòa Nhân Dân Trung Hoa và JPMorgan Chase Bank (China) Company Limited sẽ được đưa ra Ủy Ban Trọng Tài Thương Mại Và Kinh Tế Quốc Tế Trung Quốc ("**CIETAC**") để giải quyết bằng tố tụng trọng tài theo các quy tắc của CIETAC hiện hành tại thời điểm đưa ra yêu cầu giải quyết tranh chấp, địa điểm của tố tụng trọng tài là tại Bắc Kinh và tố tụng trọng tài được tiến hành bằng tiếng Anh; và (b) tranh chấp liên quan đến Khách Hàng cư trú tại Đài Loan sẽ phải tuân thủ một cách không hủy ngang thẩm quyền tài phán độc quyền của các tòa án Bang New York và Tòa Sơ thẩm Liên Bang của Hợp Chủng Quốc Hoa Kỳ tại khu Manhattan Thành Phố New York. Đối với bất kỳ tranh chấp, vụ kiện, thủ tục tố tụng hoặc thủ tục tranh tụng nào phát sinh tại Hợp Chủng Quốc Hoa Kỳ liên quan đến các Điều Khoản Dịch Vụ này, Khách Hàng đồng ý một cách không hủy ngang sẽ tuân thủ thẩm quyền tài phán độc quyền của các tòa án Bang New York và Tòa Sơ thẩm Liên Bang của Hợp Chủng Quốc Hoa Kỳ tại khu Manhattan Thành Phố New York.

7. Mobile
Di động

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.

Việc chấp nhận sử dụng dịch vụ thông báo bằng tin nhắn SMS và/hoặc kênh Truy Cập Di Động của Ngân Hàng cấu thành việc Khách Hàng cho phép Ngân Hàng gửi Dữ Liệu, tin nhắn thông báo và cảnh báo thông qua bất kỳ nhà cung cấp dịch vụ thông tin liên lạc nào, bao gồm cả các nhà cung cấp dịch vụ Internet và viễn thông, mà mỗi người này được xem như hành động trong vai trò đại diện cho Khách Hàng. Các nhà cung cấp nêu trên không được mã hóa các thông tin liên lạc.

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.

Các Người Sử Dụng Được Phép có thể phải chấp nhận thỏa thuận/hợp đồng ứng dụng hoặc thỏa thuận/hợp đồng cho phép sử dụng ứng dụng để có thể tải xuống Truy Cập Di Động. Khách Hàng xác nhận rằng trong mọi trường hợp các Tài Liệu Tài Khoản điều chỉnh việc cung cấp các dịch vụ này.

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.

Khách Hàng xác nhận rằng Ngân Hàng không chịu trách nhiệm về bất kỳ sự chậm trễ nào của bất kỳ Dữ Liệu, tin nhắn thông báo hoặc cảnh báo nào được gửi thông qua bất kỳ thiết bị di động nào.

EXHIBIT A - JURISDICTION SPECIFIC PROVISIONS
PHỤ LỤC A - CÁC QUY ĐỊNH CỤ THỂ DÀNH CHO VÙNG LÃNH THỔ CÓ THẨM QUYỀN TÀI PHÁN

A. Australia & New Zealand / Úc & New Zealand

To the extent that any supply made by the Bank under these Service Terms is a taxable supply for the purposes of the Australian Goods and Services Tax, or that goods and services tax under the New Zealand Goods and Services Tax Act 1985 is payable in respect of any supply under this License Agreement, ("**GST**"), the fees payable in respect of that taxable supply ("**original amount**") will be increased by the amount of GST payable in respect of that taxable supply. Customer must pay the increased amount at the same time and in the same manner as the original amount.

Trong chừng mực bất kỳ sự cung cấp nào được Ngân Hàng thực hiện theo các Điều Khoản Dịch Vụ này là sự cung cấp chịu thuế cho mục đích của Luật Thuế Hàng Hóa và Dịch Vụ Úc, hoặc thuế hàng hóa và dịch vụ theo Đạo Luật Thuế Hàng Hóa và Dịch Vụ New Zealand 1985 phải được nộp cho bất kỳ sự cung cấp nào theo Hợp Đồng Chuyển Quyền Sử Dụng này, ("**GST**"), thì phí phải trả đối với sự cung cấp chịu thuế đó ("**số tiền ban đầu**") sẽ được cộng thêm số GST phải nộp đối với sự cung cấp chịu thuế đó. Khách Hàng phải trả số tiền tăng thêm đó vào cùng thời điểm và theo cách thức giống như số tiền ban đầu.

B. Indonesia / In-đô-nê-xi-a

The Bank and the Customer agree that, for the effectiveness of any termination of these Service Terms or the Services provided hereunder, they hereby waive any provisions, procedures and operation of any applicable law to the extent a court order is required for the termination of these Service Terms and the Account Documentation as applicable to the services provided under these Service Terms.

Ngân Hàng và Khách Hàng thỏa thuận rằng, để bất kỳ sự chấm dứt nào của các Điều Khoản Dịch Vụ này hoặc các Dịch Vụ được cung cấp theo các Điều Khoản này có hiệu lực, Ngân Hàng và Khách Hàng thông qua đây từ bỏ bất kỳ quy định, thủ tục và sự vận dụng bất kỳ pháp luật được áp dụng nào trong chừng mực cần phải có lệnh của tòa án để chấm dứt các Điều Khoản Dịch Vụ này và Tài Liệu Tài Khoản như được áp dụng đối với các dịch vụ được cung cấp theo các Điều Khoản Dịch Vụ này.

Section 7.3 shall be replaced by "Except for losses directly resulting from errors or delay caused by the Bank's gross negligence or willful misconduct, 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."

Mục 7.3 được thay thế bằng câu sau "Ngoại trừ các tổn thất phát sinh trực tiếp từ lỗi hoặc sự chậm trễ gây ra do sự cẩu thả nghiêm trọng hoặc cố tình vi phạm của Ngân Hàng, Khách Hàng xác nhận rằng Ngân Hàng không chịu trách nhiệm về bất kỳ sự chậm trễ nào của bất kỳ Dữ Liệu, tin nhắn thông báo hoặc cảnh báo nào được gửi thông qua bất kỳ thiết bị di động nào."

C. Malaysia/Labuan / Ma-lai-xi-a/Labuan

In relation to accounts held in Malaysia (excluding Labuan) and/or where the Service is provided in Malaysia (excluding Labuan) references in the Service Terms to "Bank," shall mean J.P. Morgan Chase Bank Berhad. In relation to accounts held in Labuan and/or where the Service is provided in Labuan, references in the Service Terms to "Bank," shall mean J.P. Morgan Chase Bank, N.A., Labuan Branch. The Service provided by J.P. Morgan Chase Bank Berhad shall be accessed through http://www.jpmorganaccess.com.my and the Customer undertakes not to access or utilize or attempt to access or utilize the Service through any other JPMorgan website.

Liên quan đến các tài khoản mở tại Ma-lai-xi-a (ngoại trừ Labuan) và/hoặc trong trường hợp Dịch Vụ Được cung cấp tại Ma-lai-xi-a (ngoại trừ Labuan), dẫn chiếu trong các Điều Khoản Dịch Vụ đến thuật ngữ "Ngân Hàng" có nghĩa là J.P. Morgan Chase Bank Berhad. Liên quan đến các tài khoản mở tại Labuan và/hoặc trong trường hợp Dịch Vụ được cung cấp tại Labuan, dẫn chiếu trong các Điều Khoản Dịch Vụ đến thuật ngữ "Ngân Hàng" có nghĩa là J.P. Morgan Chase Bank, N.A., Chi Nhánh Labuan. Các dịch Vụ được cung cấp bởi J.P. Morgan Chase Bank Berhad sẽ được truy cập thông qua http://www.jpmorganaccess.com.my và Khách Hàng cam kết không truy cập hoặc sử dụng hoặc tìm cách truy cập hoặc sử dụng Dịch Vụ thông qua bất kỳ trang web của JPMorgan nào khác.

D. Republic of China (Taiwan) / Trung Hoa Dân Quốc (Đài Loan)

Section 7.3 shall be replaced by "Except for losses directly resulting from errors or delay caused by the Bank's gross negligence or willful misconduct, 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."

Mục 7.3 được thay thế bằng câu sau "Ngoại trừ các tổn thất phát sinh trực tiếp từ lỗi hoặc sự chậm trễ gây ra do sự cẩu thả nghiêm trọng hoặc cố tình vi phạm của Ngân Hàng, Khách Hàng xác nhận rằng Ngân Hàng không chịu trách nhiệm về bất kỳ sự chậm trễ nào của bất kỳ Dữ Liệu, tin nhắn thông báo hoặc cảnh báo nào được gửi thông qua bất kỳ thiết bị di động nào."

The Customer acknowledges that it will take steps to ensure it enters into the correct website before attempting to access the Service.

Khách Hàng xác nhận rằng Khách Hàng sẽ thực hiện các biện pháp để bảo đảm Khách Hàng truy cập đúng trang web trước khi nỗ lực truy cập Dịch Vụ.

E. European Union / Liên Minh Châu Âu.

The Customer acknowledges that it is not a "consumer" for the purpose of the European Union's Electronic Commerce Directive ("**ECD**") (i.e., that it is not an individual) and agrees that the Bank shall not be required to make any disclosures or do any other thing which a non-consumer may agree not to require under the UK rules and legislation implementing the ECD. For further information on the Bank, please see "Notice regarding EU e-commerce information" in the Terms & Conditions on http://www.jpmorgan.com.

Khách Hàng xác nhận rằng Khách Hàng không phải là "người tiêu dùng" cho mục đích của Chỉ Thị về Thương mại Điện tử của Liên Minh Châu Âu ("**ECD**") (cụ thể là, Khách Hàng không phải là cá nhân) và thỏa thuận rằng Ngân Hàng không phải thực hiện bất kỳ sự tiết lộ nào hoặc làm bất kỳ việc nào khác mà đối tượng không phải người tiêu dùng có thể đồng ý không yêu cầu theo các quy định và luật pháp của Vương quốc Anh về việc thi hành ECD. Để có thêm thông tin về Ngân Hàng, xin vui lòng xem "Thông báo về thông tin thương mại điện tử Liên Minh Châu Âu" trong phần các Điều Khoản và Điều kiện trên trang web http://www.jpmorgan.com.

(i) The Bank will collect information about the Customer and the Customer's employees and agents (such as, without limitation, authorized signatory details) which may constitute personal data for the purposes of the data protection law. Such personal data may be collected by or on behalf of the Bank in a number of ways (the "**Collection Methods**"), including via documentation relating to the provision to or use by the Customer of electronic banking services or via the Customer's use of such electronic banking services and via other correspondence or communications between the Customer and the Bank.

Ngân Hàng thu thập thông tin về Khách Hàng và nhân viên và người đại diện của Khách Hàng (ví dụ như, nhưng không chỉ giới hạn ở thông tin về các người ký tên được ủy quyền) mà có thể cấu thành thông tin cá nhân cho mục đích của luật bảo vệ thông tin. Các thông tin cá nhân đó có thể được thu thập bởi hoặc thay mặt cho Ngân Hàng theo nhiều cách khác nhau ("**Phương Thức Thu Thập**"), bao gồm cả thông qua tài liệu liên quan đến việc cung cấp cho Khách Hàng hoặc việc Khách Hàng sử dụng các dịch vụ ngân hàng điện tử, hoặc thông qua việc Khách Hàng sử dụng các dịch vụ ngân hàng điện tử đó, và thông qua các thư từ hoặc thông tin liên lạc khác giữa Khách Hàng và Ngân Hàng.

(ii) Details of the Bank's processing activities of personal data can be found in its EMEA Privacy Policy, which is available on the Bank's website at www.jpmorgan.com/privacy/EMEA. The Bank's EMEA Privacy Policy may be updated or revised from time to time without prior notice. The EMEA Privacy Policy may be used to assist the Customer with providing a fair processing notice to the Customer's underlying data subjects.

Thông tin về hoạt động xử lý dữ liệu cá nhân của Ngân Hàng có thể được xem tại Chính Sách Quyền Riêng Tư EMEA của Ngân Hàng, được đăng trên trang web của Ngân Hàng tại www.jpmorgan.com/privacy/EMEA. Chính Sách Quyền Riêng Tư EMEA của Ngân Hàng có thể được cập nhật hoặc sửa đổi trong từng thời điểm mà không có thông báo trước. Chính Sách Quyền Riêng Tư EMEA có thể được sử dụng để hỗ trợ Khách Hàng đưa ra thông báo xử lý thích hợp cho các đối tượng dữ liệu có liên quan của Khách Hàng.

(iii) The Customer agrees that it has an appropriate legal basis to provide personal data to the Bank and that the Customer will provide any requisite notice to individuals and ensure that there is a proper legal basis for the Bank to process the personal data as described in and for the purposes detailed in the Bank's EMEA Privacy Policy. Both the Customer and the Bank will comply with its respective obligations under applicable data protection and privacy laws.

Khách Hàng đồng ý rằng Khách Hàng có cơ sở pháp lý phù hợp để cung cấp dữ liệu cá nhân cho Ngân Hàng và rằng Khách Hàng sẽ đưa ra bất kỳ thông báo cần thiết nào cho các cá nhân và bảo đảm rằng có cơ sở pháp lý phù hợp để Ngân Hàng xử lý các dữ liệu cá nhân như được mô tả trong và cho các mục đích được nêu chi tiết tại Chính Sách Quyền Riêng Tư EMEA của Ngân Hàng. Cả Khách Hàng và Ngân Hàng sẽ tuân thủ các nghĩa vụ tương ứng của mình theo các luật áp dụng về quyền riêng tư và bảo vệ thông tin.