WELLS FARGO

South Korea

Wells Fargo International Privacy Notice

Effective: 18 September 2024

Wells Fargo Bank, N.A. Seoul Branch ("**we**", "**our**", "**us**" or the "**Company**") provides this privacy notice ("**Notice**") to describe our practices regarding the collection, storage, use, disclosure and other processing of individually identifiable information directly or indirectly identifying you or other individuals relating to your organization ("**Personal Information**"). If you or your organization has a relationship or otherwise share Personal Information with a Wells Fargo entity in any country other than South Korea, a different privacy statement at https://www.wellsfargo.com/privacy-security/ will govern the Personal Information collection and processing activities of that Wells Fargo entity.

1. Types of Personal Information Collected

Outside the United States, we primarily have relationships and accounts only with corporations and other legal entities. However, we may collect information about individual representatives ("**Individuals**") of our customer organizations ("**Customers**"), such as the Individual's:

- **Work contact details:** such as name, work address, phone number, mobile phone number, email address, and online contact details, including but not limited to unique identification and password for access to our website, mobile applications, and/or social media features.
- **Position description:** such as employer, title, position held, duties, and length of employment.
- **Authentication data:** such as passport, driver's license, resident/foreigner registration numbers and other governmental identification information, home address and telephone number, documents that verify address, date of birth, country of domicile, documents that verify employment, and signature authorization.
- **Financial data:** such as salary and other income, sources of wealth, assets and documents that verify assets, credit reports, financial relationships, and financial transactions.
- **Background check data:** such as background check information including credit and criminal checks and screening.
- **Surveillance data:** such as images and voices captured by CCTV video and audio surveillance equipment installed (to the extent permitted by local law) onto the business premises of a Wells Fargo entity if your Individuals visit the business premises.
- **Electronic and voice communications data**: such as content, data, recordings, IP addresses and session identification data relating to business communications exchanged with Wells Fargo through all applicable communication channels, including email, text, instant message or chat, transcriptions, telephonic communications, audio or video calls, communications on financial or trading platforms, voice recordings, video recordings, and presentations hosted by Wells Fargo.

Amongst the above Personal Information, some of them are considered under privacy laws in South Korea as:

- **unique identification information**, which refers to passport numbers, driver's license numbers, resident/foreigner registration numbers, and other government-issued identification information.

- **sensitive information**, which refers to information relating to an individual's ideology, belief, admission to or withdrawal from a trade union or political party, political opinions, health, sex life, DNA, criminal records, biometrics, and other personal information that is likely to markedly threaten the privacy of that individual.

Unless stated otherwise, references to Personal Information in this Notice include unique identification information and sensitive information. However, the collection, use, disclosure and processing of such information shall only be done where necessary to achieve the purposes described in Section 2 and to the extent permitted by law.

We may collect Personal Information directly from Customers or the Individuals representing the Customers, including through interactions with us and use of bank systems, private lists, and publicly available sources (such as annual reports or the public registers, databases, and websites of government entities, regulators or other authorities). Your Personal Information will be processed in accordance with South Korea's data protection laws, and only where processing is necessary to achieve the purposes described in Section 2. We may process your Personal Information in physical and electronic form and will do so in a way that adequately safeguards your Individuals' personal rights and interests in accordance with South Korea's data protection laws.

You and your Individuals have the right to refuse to consent to providing Personal Information. However, the collection and processing of Personal Information is necessary to enable the provision of services, or support the service relationship with the Customer. Failure to provide Personal Information may result in the Company being unable to provide or to continue providing services to the Customer where Personal Information is necessary for such provision.

2. Purposes of Collection and Use

The purposes of collection and use of Personal Information are:

- **To provide the services requested by our Customers**, perform obligations under our agreements, and carry out related business functions, including performing data and transaction processing, conducting credit checks, handling Customer inquiries, and managing the Customer relationship, we collect and use Personal Information including work contact details, position description, authentication data, financial data, background check data, electronic and voice communications data, and other categories of Personal Information where needed.
- **To comply with legal obligations, regulations, regulatory guidance or codes of practice** applicable to the Company and its Affiliated Entities (defined below) in the United States and/or any relevant jurisdictions, including but not limited to complying with "know your customer" obligations based on applicable anti-money laundering and anti-terrorism requirements, economic and trade sanctions, customer due diligence, fraud prevention and information security, suspicious activity reporting, foreign exchange and international trade, tax reporting and other applicable laws, regulations, ordinances, and obligations, complying with any requests from any regulator or authority to the extent permitted by applicable law, performing risk management to facilitate compliance with the above, we collect and use Personal Information including work contact details, position description, authentication data, financial data, background check data, electronic and voice communications data, and other categories of Personal Information where needed.
- **To confirm a person's authority as a representative or agent of a Customer** with which the Company or its Affiliated Entities have entered or intend to enter into various arrangements, including but not limited to deposit contracts, loan contracts, contracts for foreign exchange transactions, contracts for derivative transactions, and letters of credit, we collect and use Personal Information including work contact details, position description, background check data, authentication data, and other categories of Personal Information where needed.
- **To conduct recordkeeping and otherwise manage the business** (for example, to monitor or facilitate compliance with Wells Fargo's internal policies, to perform risk management, to maintain, improve or upgrade Wells Fargo's technology, operations or systems, raise any legal claim, defense or proceedings to protect the business, rights or property of any Wells Fargo Group entity (defined in Section 3), support the conduct of audits, support business transfers, combinations, restructuring, dissolutions or similar activities relating to any Wells Fargo Group entity,

etc.), we collect and use Personal Information including work contact details, position description, authentication data, financial data, background check data, and electronic and voice communications data, and other categories of Personal Information where needed.

3. Disclosure of Personal Information

Your Personal Information in Section 1 may be disclosed or transferred to the recipients below (which may be located outside South Korea) for the purposes listed in Section 2.

- **Affiliated Entities.** The Company has Affiliated entities operating in the United States and around the world ("**Affiliated Entities**"), including the group parent in the United States, Wells Fargo & Company, and Wells Fargo Bank, N.A. (collectively, the Company and our Affiliated Entities are the "**Wells Fargo Group**"). We may disclose Personal Information to our Affiliated Entities on a worldwide basis. Non-exhaustive lists of Affiliated Entities can be found in the following Wells Fargo & Company 10-K filings (Exhibits 21) made with the US Securities and Exchange Commission, available at the following hyperlinks:
    - https://www.sec.gov/Archives/edgar/data/72971/000007297124000064/wfc-1231x2023xex21.htm
    - https://www.sec.gov/Archives/edgar/data/72971/000007297115000449/wfc-12312014xex21.htm
- **Beneficiaries, counterparties, and other parties related to a transaction.** The Wells Fargo Group may disclose Personal Information to beneficiaries, counterparties, or other parties related to a transaction on a worldwide basis to provide the services requested by our customers and to comply with legal obligations and regulations.
- **Service providers.** The Wells Fargo Group may disclose Personal Information to information technology providers or other service providers around the world that act under our instructions regarding the processing of such data (**"Data Processors"**). Data Processors will be subject to contractual obligations to implement appropriate administrative, technical, physical, and organizational security measures to safeguard Personal Information, and to process Personal Information only as instructed. The Wells Fargo Group may also disclose Personal Information to independent external auditors or other service providers around the world that may not be acting as a Data Processor. Such service providers will be subject to any necessary contractual obligations regarding the protection and processing of such Personal Information.
- **Legal requirements.** Subject to applicable law, the Wells Fargo Group may disclose Personal Information if required or permitted by applicable law or regulation, including laws and regulations of the United States and other countries, or in the good faith belief that such action is necessary to: (a) comply with a legal obligation or in response to a request from law enforcement or other public authorities wherever the Wells Fargo Group may do business; (b) protect and defend the rights or property of any Wells Fargo Group entity; (c) act in urgent circumstances to protect the safety of Customers and their Individuals, the employees or contingent workers of any Wells Fargo Group entity, or others; or (d) protect against any legal liability. In addition, the Wells Fargo Group may share your Personal Information with U.S. regulators and with other self-regulatory bodies to which we are subject, wherever the Wells Fargo Group may do business.
- **Business transfers, combinations and related activities.** As we develop our business, the Wells Fargo Group might sell, buy, acquire, obtain, exchange, restructure, or reorganize businesses or assets. In the event of any actual or proposed sale, merger, reorganization, transaction, restructuring, dissolution or any similar event involving our business or assets, Personal Information may be shared with the relevant entity or may be part of the transferred assets and will be subject to any necessary contractual obligations to ensure the protection of Personal Information.

The recipients of Personal Information identified in this Section 3 may be in the United States or other jurisdictions outside the countries where you or your Individuals are based. As such, these overseas recipients may not be required to comply with the data protection laws of the countries where you or your Individuals are based. They may also not be required to provide you or your Individuals with comparable levels of data protection or redress under the data protection laws where you or

your Individuals are based. Some of these recipients may also act as independent data controllers (rather than Data Processors) with respect to your Personal Information. Notwithstanding the above, where required by applicable data protection laws, the Company will: (i) address any applicable requirement to ensure an adequate level of data protection before transferring Personal Information by ensuring the execution of appropriate data transfer agreements or confirming other reasonable safeguards are in place; and (ii) establish that Personal Information will be made available to recipients on a need-to-know basis only for the purposes described in Section 2 above. These measures enable us to transfer and use Personal Information in a secure manner anywhere in the world where we have an establishment or where we have contracted third parties to provide us with services.

Personal Information may be transferred electronically (e.g., by IT network, etc.) or physically (e.g., by courier, post, etc.) over the course of our relationship with the Customer and/or within the periods of retention and use explained in Section 5. You may contact us using the details in Section 8 for queries relating to offshore recipients of your Personal Information.

4. Consents

To the extent required and permitted by applicable law, you expressly consent to the collection, use, disclosure (including cross-border transfer), and other processing of Personal Information described in this Notice (as amended from time to time) by providing Personal Information to the Wells Fargo Group or authorizing our Customer to provide such information to us.

Where you directly or indirectly provide (or have provided) any Wells Fargo Group entity with the Personal Information of any individuals, you must have first informed such individuals about our data privacy practices by providing them with a copy of this Notice, and obtained all required informed consents (including separate consents) from such individuals to permit the activities described in this Notice (including subsequent modifications to the Notice described in Section 9). You expressly waive the bank secrecy or confidentiality laws and obligations, if any, of the country or countries where you and the accounts are located to the extent permitted by applicable law.

You may revoke consent for the processing of your Personal Information at any time by notifying us at the address provided in Section 8 of this Notice. Revocation of consent will not affect the lawfulness of Personal Information processing performed prior to the withdrawal request, or processing based on lawful bases other than consent. Revocation of consent may result in our inability to provide or continue to provide the requested services to the Customer where Personal Information is necessary to provide the requested services.

5. Security, Retention and Destruction of Personal Information

Security of Personal Information

Wells Fargo takes appropriate technical, physical, and organizational security measures to protect Personal Information.

- Wells Fargo's cybersecurity team, which is part of the broader technology team, provides Front Line information security risk assessment and management and is responsible for protecting the Company's information systems, networks, and data, including customer and employee data, through the design, execution, and oversight of our information security program.
- Wells Fargo has processes designed to prevent, detect, mitigate, escalate, and remediate cybersecurity incidents, including monitoring of the Company's networks for actual or potential attacks or breaches. The Company's incident response program includes notification, escalation, and remediation protocols for cybersecurity incidents, including to our Head of Technology and CISO. In addition, to help monitor and assess our exposure to ongoing and evolving risks in these areas, the Company has a cyber and information security focused risk committee led by the CISO and a technology risk committee led by the Head of Technology.

- Additional components of Wells Fargo's information security program include: (i) enhancing and strengthening of our practices, policies, and procedures in response to the evolving information security landscape; (ii) designing our information security program to align with regulatory and industry standards; (iii) investing in emerging technologies to proactively monitor new vulnerabilities and reduce risk; (iv) conducting periodic internal and third-party assessments to test our information security systems and controls; (v) leveraging third-party specialists and advisors to review and strengthen our information security program; (vi) evaluating and updating our incident response planning and protocols; and (vii) requiring employees and third-party service providers who have access to our systems to complete annual information security training modules designed to provide guidance for identifying and avoiding information security risks.
- Wells Fargo's third-party risk management program also has processes to incorporate information security and cybersecurity incident notification requirements into contracts with third-party service providers, require third parties to adhere to defined information security and control standards, and perform periodic third-party risk assessments.
- While registering with our website, mobile applications, or social media features (each, a "**Site**"), we may provide you with a unique identification and password for accessing our products and services. We encourage you to choose your password wisely such that no intruder or third party can obtain any unauthorized access to the Site. We also encourage you to keep your password confidential and not have any written or other record of the password that can be accessible by an intruder or third party.

Despite our best endeavors, unfortunately no data transmission or storage system can be guaranteed to be absolutely secure. If you have reason to believe that your interaction or Personal Information with us is no longer secure, please immediately notify us using the contact information in Section 8.

Retention of Personal Information

Your Personal Information is retained in a manner consistent with applicable law and for as long as necessary to fulfil the purposes of collection described in Section 2. Records are kept by Wells Fargo and its third-party service providers for varying periods generally ranging from 1 year to 10 years (and for longer in some cases) depending on the legal, regulatory or business requirements for the particular record. The criteria used to determine these retention periods include but are not limited to the following:

- The length of time we have an ongoing relationship with you and provide the services to you (for example, for as long as your organization has an account with us or keeps using the services);
- Whether there is a legal obligation to which we are subject (for example, certain laws require us to keep records of your transactions for a certain period of time after your organization no longer has an account with us);
- Whether retention is advisable considering our legal position (such as in regard to applicable statutes of limitations, litigation or regulatory investigations); and/or
- Whether our operational needs require maintaining your Personal Information (for example, for internal or external audits of company operations, maintaining solicitation preferences (including for former customers and non-customers), systems administration, or for fraud prevention).

Despite our best endeavors, unfortunately no data transmission or storage system can be guaranteed to be absolutely secure. If you have reason to believe that your interaction or Personal Information with us is no longer secure, please immediately notify us using the contact information in Section 8.

Procedure and Method for Destruction of Personal Information

In principle, the Company will promptly destroy the Personal Information in its possession once the Company achieves the purpose of collection and use of Personal Information. The process and means of destroying Personal Information are as follows.

Procedure: Personal Information will be transferred to a separate database (or separate document file for paper documents) and destroyed after storage for a certain period pursuant to the Company's internal policy or applicable laws and regulations (please refer to the provisions on retention and use period). Such Personal Information will not be used for any purpose other than the purpose permitted under the applicable laws and regulations.

Method: Personal Information that has been printed on paper will be shredded through the use of document shredder or incinerated. Personal Information stored in electronic file form will be deleted by using technical means that will reasonably prevent data recovery.

6. Data Subject Rights and Choice for Marketing Materials

Data Subject Rights

Your Individuals may have the following rights in relation to Personal Information we hold about them:

- Right to confirm whether their Personal Information is being processed.
- Right to be informed of processing activities relating to their Personal Information.
- Right to access and be provided with a copy of their Personal Information.
- Right to correct their Personal Information.
- Right to delete their Personal Information.
- Right to suspend the processing of their Personal Information.
- Right to refuse to accept a decision made through a fully automated processing of your Individuals' Personal Information where it impacts their rights or obligations, and a right to request an explanation of such fully automated decision-making. For clarity, as of the date of this Notice, no such fully automated decision-making is being performed by the Company.
- Right to consent, elect the scope of consent, and withdraw consent, to the processing of their Personal Information. Withdrawal of consent will not affect the lawfulness of processing done prior to withdrawal, or processing conducted on legal bases other than consent.
- Right to appropriate redress for any damage arising out of the processing of their Personal Information through a prompt and fair procedure.

Requests must be submitted by the Individual using the contact information listed in Section 8 below. After we have verified the Individual's identity, we will endeavor to respond promptly to valid data subject requests and take the other actions requested as specified by local law. Where permitted by law, we may charge an appropriate fee to cover the costs of responding to the request. These rights may not be absolute, and exceptions may be applicable. If Wells Fargo is not able to accommodate the request, the requestor will be provided with reasons for the denial.

Choice for Marketing Materials

If you do not want to receive marketing and sales materials from Wells Fargo by direct mail, telephone or email, please submit a written request using our contact details listed in Section 8 below. We will comply with your request within a reasonable period of time after receiving it or within the time period required by local law.

7. Complaints

You have a right to make a complaint if you think we have not adhered to this Notice or South Korea's data protection law in handling your Personal Information. If you would like to make a complaint, please submit your complaint in writing using the contact details in Section 8. We will respond to a written complaint within 30 days. If you are not satisfied with our

response, you may be able to pursue your complaint with the South Korean Data Protection Authority – details on how to contact the Authority are available at its website here.

8. Customer Inquiries

Please direct all requests regarding your Personal Information, or any questions regarding this Notice, to the following:

APAC Regional Privacy Officer
138 Market St, #30-01 CapitaGreen, Singapore, 048946
Telephone: (65) 6395 6900
privacy.apac@wellsfargo.com

South Korea Data Privacy Officer
Byeong-Gu Jang
Wells Fargo Bank, N.A. Seoul Branch
21/F, D1, D Tower, 17 Jong-ro 3-gil, Jongno-gu, Seoul, 03155, Korea
Telephone: (82) 2-3706-3106
Byeong-gu.jang@wellsfargo.com

9. Modifications

This Notice may be modified as a result of amendments to the law or regulations or due to other reasons. In such case, an amended Notice will be posted on our website at http://www.wellsfargo.com/privacy-security/. The page providing the Notice shall contain a date as to when the Notice was last updated.