Wells Fargo International Privacy Notice

All countries except United States, Australia, Brazil, Canada, China, Japan, New Zealand, South Korea, the United Kingdom, countries in the European Union, and Dubai International Financial Centre.

Effective: 16 August 2024

The Wells Fargo entity in Section 10 which you and/or your organization have a business relationship or otherwise share Personal Data with ("**we**", "**our**", "**us**" or "**the Company**") provides this privacy notice ("**Notice**") to describe our practices as a data controller 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 Data**"). If you or your organization have a business relationship or otherwise share Personal Data with a Wells Fargo entity in the excluded countries listed above, a different privacy notice at https://www.wellsfargo.com/privacy-security will govern the Personal Data collection and processing activities of that Wells Fargo entity.

1. Types of Personal Data Collected

Outside the United States, we primarily have relationships and accounts only with corporations and other legal entities. However, we may collect Personal Data 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, other governmental identification information, home address and telephone number, documents that verify address, date of birth, country of domicile, documents that verify employment, marriage certificate (if the Individual acts as a personal guarantor), 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, to the extent required or permitted by local law.
- **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 with Wells Fargo through all applicable communication channels, including email, text, instant message or chat, transcriptions, telephone communications, audio or video calls, voice recordings, video recordings, and presentations hosted by Wells Fargo.

IPN GEN2122 (Rev 16/08/2024)

Amongst the above Personal Data, some of them may be considered sensitive under the data protection laws applicable to the Wells Fargo entity which you have a business relationship with. What constitutes sensitive Personal Data depends on the applicable data protection law, but examples of sensitive Personal Data may include criminal records, certain types of customer financial or account information, etc. Unless stated otherwise, references to Personal Data in this Notice include sensitive Personal Data. However, sensitive Personal Data will be processed in accordance with applicable data protection laws, and only where processing is necessary to achieve the purposes described in Section 2.

We may collect Personal Data directly from Customers or the Individuals representing the Customers, including through interactions with the Bank and use of Bank systems, private lists, and publicly available sources (such as annual reports or public registers/databases/websites of government entities, regulators or other authorities). We will process your Personal Data in physical and electronic form and will do so in a way that adequately safeguards your Individuals' personal rights and interests in accordance with applicable data protection laws.

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

2. Purposes of Collection and Use

The purposes of collection and use of Personal Data 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 Data including work contact details, position description, authentication data, financial data, background check data, electronic and voice communications data, and other categories of Personal Data where needed.
- **To comply with legal obligations and 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 Data including work contact details, position description, authentication data, financial data, background check data, electronic and voice communications data, and other categories of Personal Data 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 Data including work contact details, position description, background check data, authentication data, and other categories of Personal Data where needed.
- **To conduct recordkeeping and otherwise manage the business**, such as to monitor or facilitate compliance with Wells Fargo's internal policies, to perform risk management, to support, maintain or upgrade Wells Fargo's technology, operations or systems (including in relation to cloud computing), to protect the business, rights or property of any Wells Fargo Group entity (defined in Section 3) by raising any legal claim, defense or proceedings, to 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 Data including work contact

details, position description, authentication data, financial data, background check data, electronic and voice communications data, and other categories of Personal Data where needed.

3. Disclosure of Personal Data

The Company may transfer your Personal Data in Section 1 to the recipients below 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 Data to our Affiliated Entities on a worldwide basis. A non-exhaustive list of Affiliated Entities is found in this Wells Fargo & Company 10-K filing made with the US Securities and Exchange Commission: https://www.sec.gov/Archives/edgar/data/72971/000007297124000064/wfc-1231x2023xex21.htm.
- **Beneficiaries, counterparties, and other parties related to a transaction.** The Wells Fargo Group may disclose Personal Data to beneficiaries, counterparties, or other parties related to a transaction on a worldwide basis, for example, 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 Data to information technology, cloud and other types of 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 Data, and to process Personal Data only as instructed. The Wells Fargo Group may also disclose Personal Data 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 Data.
- **Legal requirements.** Subject to applicable law, the Wells Fargo Group may disclose Personal Data 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 otherspersonal safety of Individuals, Customers, and contingent resources/employees 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 Data 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 Data 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 Data.

The recipients of Personal Data 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 data controllers (rather than Data Processors) with respect to your Personal Data. 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 Data by ensuring the execution of appropriate data transfer agreements or confirming other reasonable safeguards are in place;

and (ii) establish that Personal Data 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 Data 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.

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 Data as described in this Notice by providing Personal Data to the Wells Fargo Group or authorizing our Customer to provide such information to us. Where you directly or indirectly provide any Wells Fargo Group entity with the Personal Data 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, before providing their Personal Data to the Wells Fargo Group. 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 Data 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 Data 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 Data is necessary to provide the rquested services.

5. Security and Retention

Appropriate measures are taken so that Personal Data can be kept accurate, and up-to-date. In an effort to prevent the loss, misuse, unauthorized access, disclosure, alteration or destruction of Personal Data, Wells Fargo will take appropriate legal, technical, physical and organizational security measures to protect Personal Data. 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 Data with us is no longer secure, please immediately notify us using the contact information in Section 8.

Your Personal Data 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 data (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).

6. Data Subject Rights and Choice for Marketing Materials

Data Subject Rights

Your Individuals may have certain rights in relation to Personal Data we hold about them. These rights may vary depending on the data protection laws applicable to the Wells Fargo entity which you have a business relationship with. Your Individuals may have the right to access, correct, obtain a copy of, and be informed of the processing activities for any Personal Data held about them. They may also have the right to delete, object to, restrict processing, or seek portability of their Personal Data. They may also have the right to seek relief from data protection authorities, claim damages, seek self-defense, or commence legal proceedings for violations of their rights and interests over their Personal Data under applicable data protection laws. Finally, they have the right to consent to the processing of their Personal Data, and to withdraw any consent previously given. However, their withdrawal of consent will not affect the lawfulness of Personal Data processing performed prior to the withdrawal request, or processing based on lawful grounds other than consent.

Requests must be submitted by the Individual in writing 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 may have a right under applicable law to make a complaint if you think we have not adhered to this Notice or any applicable privacy law in handling your Personal Data. If you would like to make a complaint, please submit your complaint in writing to the contact details below most applicable to your location. 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 your data protection authority or privacy commissioner for your country.

8. Customer Inquiries

Please direct all requests relating to access, correction, and other legal rights regarding Personal Data, or any questions regarding this Notice to the location below most applicable to your location:

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

Latin America and Caribbean
Americas Regional Privacy Officer
23rd Floor, 22 Adelaide Street West
Toronto, Ontario
Canada M5H-4E3
Telephone: (416) 607-2900
Email: canadaprivacyinfo@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.

10. Wells Fargo Entities Covered by this Notice

Country	Entity Name	Address
Bermuda	Union Hamilton Reinsurance, Ltd.	2 Church Street Clarendon House Hamilton
Colombia	Wells Fargo Bank, N.A. – Santafe de Bogota, Colombia	Carrera 11 #79-35, Piso 9 Bogotá, D.C.
Hong Kong	Wells Fargo Bank, N.A. – Hong Kong Branch	1 Queens Road East, 27/F, Three Pacific Place, Wan Chai, Hong Kong
Hong Kong	Wells Fargo Securities Asia Limited	1 Queens Road East, 27/F, Three Pacific Place, Wan Chai, Hong Kong
Singapore	Wells Fargo Bank, N.A. – Singapore Branch	138 Market Street, #30-01, CapitaGreen, Singapore, 048946
Singapore	Wells Fargo CDF International Pte. Ltd.	138 Market Street, #30-02, CapitaGreen, Singapore, 048946
Singapore	Wells Fargo Securities Singapore Pte. Ltd.	138 Market Street, #30-03, CapitaGreen, Singapore, 048946
Taiwan	Wells Fargo Bank, N.A. – Taipei Branch	No.44, 17F, Chung Shan North Road, Section 2 Taipei City, Taiwan
Vietnam	Wells Fargo Bank, N.A. – Hanoi, Vietnam	No. 16, Phan Chu Trinh Street, Unit 1410, Cornerstone Building, Hoan Kiem District, Hanoi