WELLS FARGO INTERNATIONAL TEAM MEMBER PRIVACY NOTICE

This Notice applies to all countries except for the following: the United States, South Korea, the People's Republic of China-Shanghai, and those countries in the European Union, Latin America, and the Caribbean.

Effective: 23 November 2018

"**We**", "**Our**" or "**Company**" refers to the Wells Fargo entity with which you have an employment contract and which is acting as the data controller regarding the collection, use, storage, transfer, and processing of individually identifiable information about you ("**Personal Data**"). "You" or "your" refers to an individual who has an employment contract or employment relationship with the Company. This document is referred to as the "**Notice**."

Wells Fargo is one of the largest financial institutions in the world and operates globally. As described in Section 2 below, in order to carry out employment-related operations, including administering your contract or employment relationship with the Company, we need to collect, process, and use Personal Data. We also have to meet the different requirements of data protection laws across the world.
Name of group parent: Wells Fargo & Company
Headquarters location: 420 Montgomery Street; San Francisco, CA 94104 USA
Contact information for our regional Data Privacy Officers is listed in Section 7 below.

1. What Personal Data do We collect?

We may collect the following categories of Personal Data in connection with your employment to the extent permitted under applicable law:

• **Master data:** first name, middle name, and last name, personal contact details (home and mobile telephone numbers, email addresses, and home address), date and place of birth, citizenship, marital status, gender, national identification, tax, and/or social insurance number, information required for tax reporting, health insurance information, and bank account details.

• **Background data:** credit history, professional qualifications, previous addresses, prior employment history, current and past directorships held by you and members of your immediate family, education history, and professional or personal references.

• **Visa and work permit data:** copies of your passport, birth certificate, national identification card, existing and expired visa(s) and other permit details, and all such information for relevant members of your family (such as your parents, spouse, domestic/civil partner, children and/or other dependents), if required by applicable law.

• **Emergency contact information:** first name and family name, and contact information of a family member or other person to be contacted in an emergency.

• **Work contact details:** work address, work phone numbers, fax numbers, and work email address.

• **Contract data:** terms and conditions of your contract, salary or pay, and other contractual benefits such as car, educational or housing allowances; stock, incentive or bonus awards; and changes to the terms and conditions of your employment or work relationship.

• **Organizational data:** title, job position, function, employee ID, department, business unit, supervisor's name and higher level supervisor(s), cost center, signing authority, skills, work experience at the Company, user ID, and information technology access rights.

• **Employment data:** data that may be collected in the course of employment including business travel, business expenses, use of Company facilities, training activity, or attendance at Company events.

• **Computer usage data:** data about your use of equipment, electronic communications systems, and property, such as computers, mobile devices, email, internet, intranet SharePoint sites, shared drives and other data repositories and voicemail.

• **Performance data:** performance evaluations, appraisals, promotions, and assessments of performance.

• **Disciplinary data:** information about conduct, investigations, and disciplinary notices, if any.

• **Absence data:** dates of absence and reasons for absence (such as medical leave) to the extent these apply to you.

• **Benefits information:** car, mobile device, and housing allowance, contribution to health insurance, pension contribution, and the name, address, and date of birth of your spouse or domestic civil/partner, and/or dependents or children who are beneficiaries.

• **Bonus and incentive information:** details of applicable bonus, incentive and commission plans.

• **Third party data:** the name, title, employer, contact details, and location of any individual who you are related to or have a close personal relationship with who: (i) provided you with a reference for employment with Wells Fargo; (ii) is a U.S. or non-U.S. government official; or (iii) has decision making authority/capability over any matters affecting Wells Fargo.

The Company may also collect the following sensitive Personal Data as permitted by applicable law: **health-related data** (such as information on medical reports, medical questionnaires, employee health reviews and vaccines plans, workplace illness and accidents, data about sick leave processed in the course of existing employment and relevant for payroll and related tax processing, e.g., with regard to sick payment, and sickness absence management, and data relating to pregnancy), **data related to financial or investment accounts** held by you, your spouse/domestic/civil partner, your respective children (including financially independent minors) or other dependents as well as any other accounts you control, including copies of account statements and transaction details for such accounts (such as brokerage statements or other information regarding securities transactions), **criminal records data** (such as criminal records properly obtained through a lawful background reference check), **race or ethnicity-related data** (which may be apparent from processing your picture or from documents such as your passport or national identity card), or **biometric data** (such as fingerprint or voice prints) (collectively, "**Sensitive Personal Data**").

If you, for any purpose under this Notice, provide the Company with Personal Data about your spouse/domestic/civil/partner, your respective children, other dependents or other third parties, it is your responsibility to inform them of their rights with respect to such Personal Data and that you may disclose their Personal Data to the Company for these purposes. You are also responsible for obtaining the explicit consent of these individuals (unless you are authorized to provide such consent on their behalf) if such consent is required by applicable law for the collection, use, storage, transfer and processing of their Personal Data.

It is obligatory that you provide the Company with your Personal Data, without which we will not be able to process your Personal Data for the purposes set out in Section 2 below, and the administration of your employment, including the Employment Purposes (defined below), could be affected.

2. For what purposes do we use and process Personal Data?

The Company uses and processes Personal Data (via manual and electronic methods) for purposes of administering your contract with the Company and carrying out its employment relationship with you, and for purposes of managing our business operations, including complying with applicable laws and regulations on a global basis. The Company uses and processes the following categories of Personal Data for the following purposes ("**Employment Purposes**"), as permitted by applicable law.

• **To provide compensation,** including payroll, bonus, stock options, and incentives as applicable, the Company may process master data, contract data, bonus and incentive information, performance data, absence data, disciplinary data, and benefits information.

• **To provide rights, benefits, and entitlements**, and other conditions as applicable, the Company may process master data, work contact data, organizational data, contract data, bonus and incentive information, performance data, absence data, disciplinary data, benefits information, employment data, and visa and work permit data.

• **To comply with other employment-related legal requirements**, such as income tax, national insurance deductions, and applicable employment and immigration laws, the Company may process master data, work contact details, organizational data, visa and work permit data, contract data, and absence data.

• **To maintain and improve effective administration of the workforce and company facilities**, including assigning projects and tasks, conducting workforce analysis, administering project costing and estimates, managing work activities, providing performance evaluations and promotions, conducting talent management and career development, providing references as requested (if permitted by Company policy), administering learning and development training, and providing facilities management and worksite security, the Company may process work contact details, organizational data, employment data, contract data, performance data, absence data, and disciplinary data.

• **To maintain a corporate directory and offer platforms for sharing information**, including populating and making available contact details and/or an intranet website accessible by Company team members and authorized contractors to facilitate communication with you or sharing of information internally, the Company may process work contact details, organizational data, and other data you voluntarily submit for these purposes.

• **To maintain information technology ("IT") systems**, including implementing and maintaining IT systems, providing IT support and asset management, maintaining business continuity plans and processes, and managing security services and employee access rights, the Company may process work contact details, computer usage data, organizational data, and disciplinary data.

• **To monitor and assure compliance with Wells Fargo's Code of Ethics and Business Conduct, other policies and procedures, and applicable law,** including detecting or preventing possible loss or unauthorized access or processing of customer, team member, confidential or restricted data, protecting Company and other party data and assets, mitigating insider trading risk, avoiding actual or perceived conflicts of interest, and meeting regulatory expectations, conducting internal audits and investigations, handling any potential or other claims, and engaging in disciplinary actions and terminations, the Company may process work contact details, organizational data, contract data, bonus and incentive information, absence data, benefits information, performance data, employment data, background data, third party data, Sensitive Personal Data, computer usage data, and disciplinary data.

• **To respond to requests and legal demands from regulators or other authorities**, including complying with requests from regulators or other authorities in your home country or other jurisdictions, such as attachment of earnings orders, and participating in legal proceedings including domestic and cross-border litigation and discovery procedures, the Company may process work contact details, organizational data, contract data, bonus and incentive information, performance data, background data, third party data, Sensitive Personal Data, computer usage data, disciplinary data, employment data, and any other category of Personal Data necessary to respond to the request or legal demand.

• **To notify you or your family or emergency contacts in the event of any emergencies**, the Company may process master data and emergency contact information.

• **To perform certain limited activities with respect to Sensitive Personal Data**, including calculating the number of sick days for statutory wage tracking, reporting workplace accidents as required by applicable law, complying with obligations to make reasonable adjustments and other disability discrimination legislation, monitoring equal opportunities, confirming someone's right to work, assessing their suitability for a position,

verifying identity for security purposes, and complying with other applicable law, the Company may process Sensitive Personal Data.

The Company will not process Personal Data for any purpose incompatible with the purposes outlined in this section, unless it is required or permitted by applicable law, or as authorized by you. For some activities, processing of certain Personal Data continues after individuals have left the service of the Company. The Company's general practice is not to keep Personal Data longer than necessary for the fulfillment of the purposes outlined in this section, in accordance with our standard records retention periods, or as required or appropriate in the jurisdiction where such records or information is retained. However, we may need to hold Personal Data beyond these time periods due to regulatory requirements of a particular country or in response to a regulatory audit, investigation or other legal matter. These requirements also apply to our third party service providers.

3. Under what conditions is Personal Data transferred to recipients in different countries?

Wells Fargo operates across the globe, and we may transfer Personal Data for Employment Purposes to Wells Fargo entities located in other countries. This can also happen when we engage third parties to assist us with certain operations and activities, as they also may be established in different countries.

We have put in place measures to enable the transfer of Personal Data to another country in accordance with applicable law regardless of the global location of our entities. These measures enable us to transfer and use Personal Data in a secure manner anywhere in the world where we have operations, or where we have contracted third parties to provide us with services. The countries where we have operations are shown on this map at www.wellsfargo.com/com/international/locations. We may also transfer Personal Data to other countries where our third party service providers are located.

The Company may transfer Personal Data to third parties for Employment Purposes as follows:

Wells Fargo U.S. Since management, human resources, legal and audit responsibility partially rests with Wells Fargo & Company as the group parent in the United States ("**Wells Fargo & Company**") and with Wells Fargo Bank, N.A. operations in the U.S. ("**Wells Fargo Bank, N.A.**") (collectively, "**Wells Fargo U.S.**"), the Company may transfer Personal Data to, or otherwise allow access to such data by, Wells Fargo U.S., which may use, transfer, and process the data for the following purposes: to maintain and improve effective administration of the workforce; to provide rights, benefits, stock grants, and entitlements; to maintain a corporate directory; to maintain IT systems; to monitor and assure compliance with Wells Fargo's Code of Ethics and Business Conduct, other policies and procedures, and applicable law; and to respond to requests and legal demands from regulators and other authorities, including such authorities in the United States.

• **Affiliated Entities.** To the extent that your management or human resources responsibility for overseeing your employment relationship with the Company partially rests with different Wells Fargo entities ("**Affiliated Entities**"), the Company may also transfer Personal Data to, or otherwise allow access to such data by, relevant Affiliated Entities, which may use, transfer, and process the data for the following purposes: to maintain and improve effective administration of the workforce; to provide rights, benefits, stock grants, and entitlements, to maintain a corporate directory; to maintain IT systems; to monitor and assure compliance with Wells Fargo's Code of Ethics and Business Conduct, other policies and procedures, and applicable law; and to respond to requests and legal demands from regulators and other authorities, including authorities in the jurisdictions where the Affiliated Entities are located. See Exhibit 21 to the most recent Form 10-K we filed with the U.S. Securities and Exchange Commission at www.sec.gov/Archives/edgar/data/72971/000007297118000272/wfc-

12312017xex21.htm for a select list of Affiliated Entities and subsidiaries as of December 31, 2017.

• **Customers and Prospects.** As necessary in connection with business operations, work contact details may be transferred to customers and other third parties as permitted by applicable law.

• **Regulators, authorities, and certain third party controllers.** As necessary for the Employment Purposes described above, Personal Data may be transferred to regulators, courts, and other authorities (e.g., tax and law enforcement authorities), and the Wells Fargo & Company Board of Directors.

• **Acquiring entities.** If the Wells Fargo business for which you work is sold or transferred in whole or in part (or such a sale or transfer is being contemplated), your Personal Data may be transferred to the new employer or potential new employer, subject to any rights provided by applicable law, including to such new or potential new employers in the jurisdictions and other countries where these entities are located.

• **Service providers.** As necessary for the Employment Purposes described above, Personal Data may be shared with one or more parties, whether affiliated or unaffiliated, to process Personal Data under appropriate instructions ("**Data Processors**"). Such Data Processors may carry out instructions related to IT system support, payroll, training, compliance, and other activities, and will be subject to contractual obligations to implement appropriate technical and organizational security measures to safeguard the Personal Data, and to process the Personal Data only as permitted by the contract. In addition, to the extent that Personal Data is disclosed to independent external auditors, benefits providers, insurance carriers, or other service providers that may not be acting solely as a Data Processor, such service providers will be subject to any necessary contractual obligations regarding the protection and processing of such information.

The recipients of Personal Data identified in this Section 3 may be located in the United States and other jurisdictions that may not provide the same level of data protection as your home country. To the extent required by applicable law, the Company, Wells Fargo U.S., and Affiliated Entities will: (i) address any applicable requirement to assure an adequate level of data protection before transferring Personal Data by assuring the execution of appropriate data transfer agreements or confirming other controls or otherwise provide appropriate safeguards regarding transfers of Personal Data to other countries; and (ii) establish that Personal Data will be made available to individuals within the recipient entities on a need-to-know basis only for the relevant Employment Purposes described above. Please contact the applicable regional Data Privacy Officer, using the contact information in Section 7, to obtain additional information about these safeguards.

4. What security measures does the Company implement?

Personal Data will be safely stored in the databases of Wells Fargo and will be held and maintained by Wells Fargo or on behalf of Wells Fargo by Wells Fargo service providers. The Company has implemented appropriate technical, physical and organizational security measures to safeguard Personal Data in accordance with the Company's Information Security Policy and standards. When we retain a non-affiliated entity or service provider to perform a function, that entity will be required to protect workers' Personal Data in accordance with our standards.

5. What are my rights in relation to Personal Data?

You may have certain rights under applicable law that enable you to have control and oversight over what organizations do with your Personal Data. These rights may include the right to seek relief from data protection authorities and the right to request access, correction, suspension of use, or deletion of your Personal Data. If you have questions about your Personal Data rights, or whether different local laws apply, please contact the applicable regional Data Privacy Officer using the contact information in Section 7 below.

In addition to the regional Data Privacy Officers listed in Section 7 below, the Company has appointed a contact person ("**Contact Person**") to respond to your questions and complaints. The Contact Person is generally the Human Resources Manager at the Company or, if there is no Human Resources Manager, the Branch Manager or Country Manager for that location.

6. Under what circumstances are equipment, electronic communication systems, and property subject to monitoring?

To the extent permitted by applicable law, and subject to any other local notices or policies, the Company reserves the right to monitor the use of equipment, electronic communication systems, and property, including original and backup copies of email, instant messaging, text messaging, voicemail, internet use, computer use activity, and CCTV. The Company may engage in such activities to administer IT access, provide IT support, manage security services and employee authorizations, as well as to monitor and assure compliance with Wells Fargo's Code of Ethics and Business Conduct, and other Company policies and procedures. You should not expect privacy in connection with your use of any equipment, systems, or property, including personally-owned equipment to the extent subject to Company Bring Your Own Device ("**BYOD**") policies. Wells Fargo also maintains separate policies that govern BYOD, including when and how Wells Fargo may perform monitoring. If you use a BYOD approved device, you should review those policies.

Even if you create or have access to passwords to protect against unauthorized access to correspondence and activities, using that password does not make the related communications or activities private. In addition, phone calls made or received on any business telephone may be monitored or recorded for regulatory and compliance purposes. Monitoring may be conducted remotely or locally, and related Personal Data collected and processed by the Company, Wells Fargo U.S., Affiliated Entities, and/or Data Processors using software, hardware or other means. Personal Data obtained through monitoring may be transferred to regulators and other authorities, as well as the Wells Fargo & Company Board of Directors, and other recipients as necessary for the purposes described above, including recipients in your home country or other jurisdictions. Personal Data obtained through monitoring will be safeguarded in accordance with the security measures set out in Section 4 above. Personal Data obtained through monitoring, which is relevant to the purposes described above, will be retained for the time periods described in Section 2 above subject to any rights team members may have under applicable law.

When carrying out monitoring of use of our equipment or systems (including emails and phone calls) it will not normally be the Company's intention to access any Personal Data (except where it is relevant to the purposes described above), and we shall use our reasonable endeavors not to access, copy or use any Personal Data unless necessary. If such access occurs inadvertently, and it is not relevant to the purposes, we shall delete any and all such Personal Data as soon as it comes to our attention.

7. How do I contact a Data Privacy Officer for questions?

The Company has appointed regional Date Privacy Officers (as listed below) who are responsible for responding to requests in relation to your Personal Date.

Canada:
Americas Regional Data Privacy Officer
MAC O1038-230
23rd Floor, 22 Adelaide Street West
Toronto, Ontario
Canada M5H-4E3
Telephone: (416) 775-2900
canadaprivacyinfo@wellsfargo.com

APAC Region excluding India and the Philippines:
APAC Regional Data Privacy Officer
MAC O2008-010
Cityplaza Four, 12 Taikoo Wan Road
Quarry Bay, Hong Kong
Telephone: (852) 2509-6335
privacy.apac@wellsfargo.com

India Grievance Officers:
Wells Fargo Bank N.A. Mumbai
Representative Office
Shukyi Yun
shuki.yun@wellsfargo.com
Wells Fargo EGS (India) Private Limited
Prasanth P
prasanth.p@wellsfargo.com

Philippines Data Privacy Officers:
Wells Fargo Bank N.A.
Manila Representative Office
Maxwell Leveson, Data Privacy Officer
MAC O2008-010
Cityplaza Four, 12 Taikoo Wan Road
Quarry Bay, Hong Kong
Telephone: (852) 2509-6335
maxwell.leveson@wellsfargo.com

Wells Fargo Enterprise Global Services, LLC
Jacqueline Almero, Data Privacy Officer
MAC O2037-020
1180 Wells Fargo Drive, 11 Le Grand Avenue
McKinley Hill, Dr. Taguig, Philippines
Telephone: (63) 908-863-9467
jacqueline.s.almero@wellsfargo.com

Acknowledgement and Consent

I understand that the Company will collect, use, process, store and transfer Personal Data as described in this Notice. By signing below or clicking the accept button, if acknowledged electronically, I confirm my consent to the collection, use, processing, storage and transfer of Personal Data in accordance with the terms and conditions contained in this Notice. I also consent to the transfer of my Personal Data outside my country of residence as described in this Notice. I agree that this Notice and Consent supersede any prior notice on this subject and shall cover all Personal Data collected or maintained by the Company in connection with my employment. I understand that I may decline to provide my Personal Data, but I may not be able to receive certain employment services described in this Notice, including but not limited to payment of salary and bonus, provision of insurance and other benefits.

Name: ASRAR FAROOQ BHAT

Emp Id:

Date: 21/08/2022

Signature: