State Bank of India
(California)

EMPLOYEE NOTICE OF COLLECTION

Under the California Consumer Privacy Act of 2018 (CCPA) California residents have the right to know and delete the categories of personal information their employer collects about them and the purpose for the collection. On November 3, 2020, Californians approved the California Privacy Rights Act (CPRA), which grants California consumers additional rights, including rights to correct inaccurate personal information, right to limit the use and disclosure of sensitive personal information, right to access information in readily usable format. The Employee Notice of Collection explains the types of personal information State Bank of India (CA) may collect about its employees, job applicants, and contractors in the ordinary course of business and how that information may be used. Privacy is the Bank's priority, and every reasonable effort is made to protect the information the Bank holds on its employees.

INFORMATION COLLECTED

The Bank collects information that identifies, relates to, describes, references, is a reasonably capable of being associated with, or could reasonably linked be (directly or indirectly) with a particular individual, household, or devise ("Personal Information").

Personal information may be collected directly from you, indirectly from you, including, but not limited to our website, your mobile devise, through email, in physical locations, through the mail and/or over the telephone. The following categories of Personal Information may be collected from job applicants, employees, or contractors, which will depend on the particular business purpose for which we collect it:

CATEGORY	PURPOSE
Identifiers: Name, alias, postal address, telephone number, unique personal identifier, Social Security Number, date of birth, place of birth. Driver's license number, state identification number, passport, or visa number	Manage and document employment and related actions with us. Maintain employee information in Bank directories. Administer employee engagement programs. Use Bank communication tools such as video conferencing. Administer occupational safety and health programs. Protect the safety and security of our employees; guests; property and assets including monitoring activities on our premises and activity using our computers, devices, networks, communications and other assets and resources. Detect security incidents and other fraudulent activity. Investigate and respond to claims. Comply with applicable laws (i.e., health and safety, employment laws). Use in ways disclosed for our business activities.
Professional and Employment-Related Information: ➢ Employer(s) ➢ Employment History ➢ Salary/Income and bonus data	To support employment, infrastructure, and human resources management, including providing benefits to employees and dependents, healthcare and retirement plans, manage pay and compensation activities,

➢ Background check and criminal history ➢ Performance and disciplinary records ➢ Leave of absence information ➢ Employee Wellness Screening Information	manage and operate our facilities and infrastructure, and process employment applications; protect the safety and security of our workforce, guests, property and assets including monitoring our facilities and activity using our computers, devices, networks, communications, and other assets and resources; detect security incidents and other fraudulent activity; investigate and respond to claims; comply with applicable laws (i.e. health and safety, employment laws) and use in ways disclosed for our business activities.
Education Information: ➢ Schools Attended ➢ Dates of Attendance ➢ Honors and Awards Received	To support employment, infrastructure, and human resources management, including providing benefits to employees and dependents, healthcare and retirement plans, manage pay and compensation activities, manage and operate our facilities and infrastructure, and process employment applications; protect the safety and security of our workforce, guests, property and assets including monitoring our facilities and activity using our computers, devices, networks, communications, and other assets and resources; detect security incidents and other fraudulent activity; investigate and respond to claims; comply with applicable laws (i.e. health and safety, employment laws) and use in ways disclosed for our business activities.
Record Information: Information we maintain in our recruitment, employment, contractor, and other similar records. ➢ Signature ➢ Physical characteristics or description ➢ Telephone number ➢ Bank Account Number ➢ Credit Card Number, ➢ Debit Card Number or any other financial information ➢ Medical or health insurance information (including insurance policy number, subscriber identification number, application history, claim history, appeal records.)	Manage and document employment and related actions with us. Maintain employee information in Bank directories. Administer employee engagement programs. Use Bank communication tools such as video conferencing. Administer occupational safety and health programs. Protect the safety and security of our employees; guests; property and assets including monitoring activities on our premises and activity using our computers, devices, networks, communications and other assets and resources. Detect security incidents and other fraudulent activity. Investigate and respond to claims. Comply with applicable laws (i.e., health and safety, employment laws) and use in ways disclosed for our business activities.
Legally Protected Characteristics: Information considered "protected classification" under California or Federal Law ➢ Age ➢ Race/Ethnicity	Manage and document employment and employment related actions with us, such as requests for reasonable accommodations related to disability or religion. Maintain emergency contact and beneficiary details.

➢ Citizenship ➢ Marital Status ➢ Medical Condition ➢ Military Status ➢ Sex (including gender, gender identity, sexual orientation, gender expression, pregnancy, childbirth, and/or any other medical condition) ➢ Physical or mental disability ➢ Or Religion to the extent disclosed by the employee	Comply with applicable laws (i.e., health and safety, employment laws) and used in ways disclosed for our business activities.
Biometric Information: Information regarding your physiological, biological, or behavioral characteristics that can be used to identify you.	Obtain access to certain Bank physical structures and facilities.
Internet and other electronic network activity information: All activity on the Bank's information systems, such as IP address, internet browsing history, search history, intranet activity email communications, social medial postings, stored documents and emails, usernames, and passwords. All activity on communications systems including phone calls, call logs, voice mails, text messages, chat logs, app use, mobile browsing and search history, mobile email communications, and other information regarding an employee's use of Bank issued devices and certain Bank information that is accessed or stored on employee's personal devices that are used for Bank business.	To facilitate the efficient and secure use of the Bank's employment processes and management including providing benefits to employees and dependents, including healthcare and retirement plans.
Geolocation Data: Information that can be used to identify the physical location of devices, assets or resources that are managed by the Bank.	To facilitate the efficient and secure use of the Bank's employment processes and management including providing benefits to employees and dependents, including healthcare and retirement plans.
Environmental Information: Information that is typically detected by the senses. ➢ Audio ➢ Electronic, ➢ Visual ➢ Thermal, or Olfactory information	Maintain employee information in Bank directories. Use Bank communication tools such as video conferencing. Use in ways disclosed for our business activities.
Inferences Drawn from the Information Identified Above: ➢ Preferences ➢ Characteristics ➢ Behavior ➢ Attitudes ➢ Abilities	To facilitate the efficient and secure use of the Bank's employment processes and management including providing benefits to employees and dependents, including healthcare and retirement plans.

Categories of Sensitive Personal Information (SPI) We Collect: ➢ Social Security Number ➢ State Identification Number ➢ Driver's License Number ➢ Passport Number ➢ User ID ➢ Password ➢ Security Questions ➢ Access Code ➢ Geolocation ➢ Racial or Ethical Origin ➢ Content of mail, email and text messages ➢ Biometric Identification Information ➢ Health Information	

SOURCES OF INFORMATION COLLECTED

The Bank obtains the above listed categories of Personal Information from the following potential sources:

- Directly from employees, when establishing an account, deposit, loan, or any related services the Bank may offer.
- Third-party reports, such as credit reports, account reporting or identify verification services.
- Third-party organizations or companies that provide data that support the Bank's products and services, such as fraud prevention, underwriting, business management and our everyday operation.

Personal information does not include:

- De-identified or aggregated consumer information.
- Public records or generally available sources, including those from federal, state, and local government entities, we well as the media.
- Information excluded from the scope of the CCPA:
    - Health or medical information covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the California Confidentiality of Medical Information Act (CMIA).
    - Personal information covered by certain sector-specific privacy laws, including the Fair Credit Reporting Act (FCRA) and the Gramm-Leach-Bliley Act (GLBA) or California Financial Information Privacy Act (FIPA), and the Driver's Privacy Protection Act of 1994.

DISCLOSURE OF PERSONAL INFORMATION

The Bank may disclose Personal Information for any of the purposes described above. Although the Bank is not liable for third-party malfeasance regarding Personal Information, the Bank will make reasonable attempts to ensure that third parties used will safeguard Personal Information and will use it only for the purpose outlined and authorized by the Bank.

Personal Information may be disclosed to the following:

- Third-party Service Providers: Paychex, Empower Retirement, Pentegra Retirement Services, Playa Vista Insurance, Anthem, Health Net, AFLAC, Nationwide, Blue Vision, W/C Insurance, Horizon
- Other Bank-affiliated service providers who facilitate employment-related functions and are disclosed to employees in advance: Indeed, ZipRecruiter, US Background Screening
- Government or regulatory agencies as required by law, including public health officials who may request information regarding COVID-19.

SALE, SHARE AND RETENTION OF PERSONAL INFORMATION

The Bank does not engage in the sale or share (as defined by CPRA) of Personal Information related to employees, applicants, or consultants. The Bank will retain the information as long as it is reasonably necessary for each disclosed purpose.

PRIVACY RIGHTS UNDER THE CALFOIRNIA CONSUMER PRIVACY ACT

For further information, please refer to the State Bank of India's (California) California Consumer Privacy Act Privacy Policy (www.sbical.com/privacy).