FIRST NORTHERN BANK

PRIVACY NOTICE TO CALIFORNIA JOB APPLICANTS

First Northern Bank and/or any affiliated entities (collectively, the "**Company**" or "**we**") provide this California Privacy Notice ("**Notice**") to describe our privacy practices with respect to our collection of Personal Information as required under the California Consumer Privacy Act ("**CCPA**"). This Notice applies only to job applicants and candidates for employment who are residents of the State of California and from whom we collect "**Personal Information**" as defined in the CCPA.

1. Information We Collect From or About Job Applicants

We may collect Personal Information from you in a variety of different situations and using a variety of different methods, including, but not limited to, on our website, your mobile device, through email, in physical locations, through written applications, through the mail, and/or over the telephone. Generally, we may collect, receive, maintain, and use the following categories of Personal Information, depending on the particular purpose and to the extent permitted under applicable law. The examples provided for each category are not intended to be an exhaustive list or an indication of all specific pieces of information we collect from or about you in each category, but rather the examples are to provide you a meaningful understanding of the types of information that may be collected within each category.

CATEGORY	EXAMPLES	Retention Period
Personal Identifiers	Name, alias, social security number, driver's license or state identification card number, passport number.	If hired, then name will be retained permanently, and the rest will be retained for duration of employment plus 6 years. If not hired, it will be retained for 4 years from when position is filled or the date we receive your information, whichever is longer.
Contact Information	Home, postal or mailing address, email address, home phone number, cell phone number.	If hired, this data will be retained permanently. If not hired, it will be retained for 4 years from when position is filled or the date we receive your information, whichever is longer.
Pre-Hire Information	Information provided in your job application or resume, information gathered as part of background screening and reference checks, pre-hire drug test results, information recorded in job interview notes by persons conducting job interviews for the Company, information contained in candidate evaluation records and assessments, information in work product samples you provided, and voluntary disclosures by you.	If hired, this data will be retained for duration of employment plus 6 years. If not hired, it will be retained for 4 years from when position is filled or the date we receive your information, whichever is longer.

Employment History	Information regarding prior job experience, positions held, and when permitted by applicable law your salary history or expectations.	If hired, this data will be retained for duration of employment plus 6 years. If not hired, it will be retained for 4 years from when position is filled or the date we receive your information, whichever is longer.
Education Information	Information contained in your resume regarding educational history and information in transcripts or records of degrees and vocational certifications obtained.	If hired, this data will be retained for duration of employment plus 6 years. If not hired, it will be retained for 4 years from when position is filled or the date we receive your information, whichever is longer.
Internet, Network, and Computer Activity	Internet or other electronic network activity information related to a job applicant's usage of Company networks, servers, intranet, or Company-owned computers and electronic devices, including system and file access logs, security clearance level, browsing history, search history, and usage history.	2 years unless related to category of data that requires a longer retention period
Mobile Device Security Information	Data identifying a job applicant's device accessing Company networks and systems, including cell phone make, model, and serial number, cell phone number, and cell phone provider.	2 years unless related to category of data that requires a longer retention period
Online Portal and Mobile App Access and Usage Information	Where job applicant or candidate must create an account to apply for a job, collect the applicant's username and password, account history, usage history, and any information submitted through the account.	2 years unless related to category of data that requires a longer retention period

Of the above categories of Personal Information, the following are categories of Sensitive Personal Information the Company may collect:

1. Personal Identifiers (social security number, driver's license or state identification card number, passport number)
2. Account Information (your Company account log-in, in combination with any required security or access code, password, or credentials allowing access to the account)
3. Medical and Health Information

Personal information ***does not*** include:

- Publicly available information from government records.
- Information that a business has a reasonable basis to believe is lawfully made available to the general public by the job applicant or from widely distributed media.

- Information made available by a person to whom the job applicant has disclosed the information if the job applicant has not restricted the information to a specific audience.
- De-identified or aggregated information.

2. How We Use Personal Information and Sensitive Personal Information

The Personal Information and Sensitive Personal Information we collect, and our use of Personal Information and Sensitive Personal Information, may vary depending on the circumstances. This Notice is intended to provide an overall description of our collection and use of Personal Information and Sensitive Personal Information. Generally, we may use or disclose Personal Information and Sensitive Personal Information we collect from you or about you for one or more of the following purposes:

1. To fulfill or meet the purpose for which you provided the information. For example, if you share your name and contact information to apply for a job with the Company, we will use that Personal Information in connection with your candidacy for employment.
2. To comply with local, state, and federal law and regulations requiring employers to maintain certain records (such as immigration compliance records, accident or safety records, and tax records).
3. To evaluate, make, and communicate decisions regarding your job application and candidacy for employment.
4. To obtain and verify background checks, references, and employment history.
5. To communicate with you regarding your candidacy for employment.
6. To permit you to create a job applicant profile, which you can use for filling out future applications if you do not get the job you are applying for.
7. To keep your application on file even if you did not get the job applied for, in case there is another position for which we want to consider you as a candidate even if you do not formally apply.
8. To evaluate and improve our recruiting methods and strategies.
9. To engage in lawful monitoring of job applicant activities and communications when they are on Company premises, or utilizing Company internet and WiFi connections, computers, networks, devices, software applications or systems.
10. To engage in corporate transactions requiring review or disclosure of job applicant records subject to non-disclosure agreements, such as for evaluating potential mergers and acquisitions of the Company.
11. To evaluate, assess, and manage the Company's business relationship with vendors, service providers, and contractors that provide services to the Company related to recruiting or processing of data from or about job applicants.
12. To improve job applicant experience on Company computers, networks, devices, software applications or systems, and to debug, identify, and repair errors that impair existing intended functionality of our systems.
13. To protect against malicious or illegal activity and prosecute those responsible.
14. To prevent identity theft.
15. To verify and respond to consumer requests from job applicants under applicable consumer privacy laws.
16. **INFECTIOUS DISEASE PURPOSES (pandemic, outbreak, public health emergency, etc.)**
    a. To reduce the risk of spreading the disease in or through the workplace.
    b. To protect job applicants and other consumers from exposure to infectious diseases (e.g., COVID-19).
    c. To comply with local, state, and federal law, regulations, ordinances, guidelines, and orders relating to infectious diseases, pandemics, outbreaks, and public health emergencies, including applicable reporting requirements.

d. To facilitate and coordinate pandemic-related initiatives and activities (whether Company-sponsored or through the U.S. Center for Disease Control and Prevention, other federal, state and local governmental authorities, and/or public and private entities or establishments, including vaccination initiatives).
e. To identify potential symptoms linked to infectious diseases, pandemics, and outbreaks (including through temperature checks, antibody testing, or symptom questionnaire).
f. To permit contact tracing relating to any potential exposure to infectious diseases.
g. To communicate with job applicants and other consumers regarding potential exposure to infectious diseases (e.g., COVID-19) and properly warn others who have had close contact with an infected or symptomatic individual so that they may take precautionary measures, help prevent further spread of the virus, and obtain treatment, if necessary.

3. Retention of Personal Information

The Company will retain each category of personal information in accordance with our established data retention schedule as indicated above. Some of the retention periods in the retention schedule above are measured from a particular point in time that has not occurred yet, such as the end of employment or end of a relationship (whether business, contractual, or transactional) plus a certain number of years. Where no particular event is defined in the retention schedule as the point from which the retention period is measured, we will measure the retention period from either (1) the date the record or data was collected, created, or last modified, (2) the date of the particular transaction to which the record or data pertains, or (3) another triggering event that is determined to be reasonable and appropriate based on the nature of the data and the legal/business needs for its continued use.

In deciding how long to retain each category of personal information that we collect, we consider many criteria, including, but not limited to: the business purposes for which the Personal Information was collected; relevant federal, state and local recordkeeping laws; applicable statutes of limitations for claims to which the information may be relevant; and legal preservation of evidence obligations.

We apply our data retention procedures on an annual basis to determine if the business purposes for collecting the personal information, and legal reasons for retaining the personal information, have both expired. If so, we will purge the information in a secure manner.

4. Sale/Sharing of Information to Third Parties

The Company does **not** and will not sell your Personal Information or Sensitive Personal Information for any monetary or other valuable consideration. The Company does **not** and will not share your Personal Information or Sensitive Personal Information for cross-context behavioral advertising.

5. Access to Privacy Policy

For more information, please review the Company's Privacy Policy at https://www.thatsmybank.com/privacy-policy.html

By finalizing and submitting my application, I acknowledge and confirm that I have received and read and understand this disclosure.