

CALIFORNIA CONSUMER PRIVACY ACT NOTICE

Updated February 22, 2022

- I. Your Rights**
- II. What Personal Information is Covered?**
- III. What Personal Information is Not Covered?**
- IV. Your Choices**
- V. Our Personal Data Collection and Disclosures**

I. YOUR RIGHTS

The California Consumer Privacy Act ("CCPA") grants California residents ("consumers") or another person authorized to act on behalf of the consumer, the right to:

- A. Know what personal information Bank of the West, a California banking corporation and its wholly-owned subsidiaries, including BancWest Investment Services (collectively, "Bank of the West" or the "Bank"), has collected about you during the prior twelve months;
- B. Know whether Bank of the West sells your personal information, and if so, to whom;
- C. Give or withhold consent for Bank of the West to sell your personal information;
- D. Request that Bank of the West disclose to you:
 - 1. The categories of personal information the Bank has collected about you;
 - 2. The categories of sources from which the personal information is collected;
 - 3. The purpose for collecting the personal information;
 - 4. The categories of third parties with whom the Bank shares personal information, and
 - 5. The specific pieces of personal information that the Bank has collected about you;
- E. Request that Bank of the West delete your personal information, to the extent possible; and
- F. Receive non-discriminatory services and product pricing from Bank of the West, regardless of whether you exercise your privacy rights under the CCPA.

Please note that identities of individuals requesting deletion or disclosure of their personal information must first be verified to protect you and the Bank from fraud and identity theft. Please note that the Bank may not disclose or delete all personal information requested by consumers due to various state and federal regulations governing financial institutions and available statutory exemptions.

II. WHAT PERSONAL INFORMATION IS COVERED?

Personal information is defined under the CCPA to include any information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked with a particular consumer or household. Examples include social security numbers, account information, transaction histories, credit information, and biometric data.

III. WHAT PERSONAL INFORMATION IS NOT COVERED?

Much of the personal information that the Bank collects is already regulated by federal and state laws, and therefore is exempt from the CCPA. For instance, the CCPA does not apply to personal information collected or disclosed in connection with financial products or services that are used primarily for personal, family, or household purposes. For information regarding how Bank of the West uses personal information collected in connection with these financial products or services, please see the Bank's [Consumer Privacy Policy](#). The CCPA also does not apply to information that is governed by the privacy, security and breach notification rules issued by the U.S. Department of Health and Human Services pursuant to Health Insurance Portability and Accountability Act, or certain personal information collected or disclosed by a consumer reporting agency pursuant to the Fair Credit Reporting Act. Currently, the CCPA does not apply to personal information that reflects a communication or transaction between the Bank and another company, partnership, sole proprietorship, non-profit, or government agency, so long as that communication or transaction involves due diligence about the Bank or other business, or the Bank is providing or receiving a product or service. The CCPA also currently does not afford access or deletion rights to you if your information was collected and used by the Bank in the context of your role as a job applicant, employee, director, officer, medical staff member, or contractor of the Bank.

IV. YOUR CHOICES

Currently, Bank of the West does not sell personal information. If in the future, Bank of the West seeks to sell the personal information of California residents, it will provide notice and opportunity to opt-out. By default, California residents the Bank knows to be under the age of 16 would be opted out of the sale of their personal information.

If you would like to request a disclosure of your personal information collected by Bank of the West, you may do so by calling the toll-free number 1-844-377-3337 or TTY 1-800-659-5495 or by going to <https://www.bankofthewest.com/ccpa>.

If you would like to request that the Bank delete your personal information, you may do so by calling the toll-free number 1-844-377-3337 or TTY 1-800-659-5495 or by going to <https://www.bankofthewest.com/ccpa>. Please note that not all personal information is eligible to be deleted. For example the Bank may retain personal information in order to:

- A. Complete transactions or services for which the information was collected or reasonably anticipated, or provide a service requested by the consumer;
- B. Detect security incidents and protect against malicious, deceptive, fraudulent, or illegal activity and prosecute those responsible for such activity;
- C. Debug or identify errors;
- D. Exercise free speech, or allow other consumers to do the same;
- E. Comply with certain sections of the California Electronic Communications Privacy Act;
- F. Engage in certain types of research where the consumer has provided informed consent;
- G. Enable solely internal uses reasonably aligned with consumer expectations;
- H. Comply with a legal obligation; or
- I. Otherwise use it internally in a lawful manner that is compatible with the context in which the consumer provided the information.

In order to make a request for the Bank to disclose or delete your personal information, you must first authenticate your identity by providing certain pieces of personal information, which may include name, mailing address, state of residence, date of birth, e-mail address, phone number, and the last four digits of your social security number, and completing a knowledge-based authentication challenge. While not all pieces of personal information requested are mandatory, the inclusion of optional personal information will assist the Bank in completing your request.

Authorized agents may make a request on behalf of a California resident by contacting us at 1-844-377-3337 or TTY 1-800-659-5495. Authorized agents must authenticate their identity, the identity of the consumer on whose behalf they are making the request, and their authority to act on the consumer's behalf.

V. OUR PERSONAL DATA COLLECTION AND DISCLOSURES

Bank of the West collects individual identifier, protected classification, commercial, biometric, network activity, geolocation, audio, electronic, visual, professional, employment-related, education, and consumer profile information for a variety of business purposes, including to make credit decisions, finance the Bank, prevent fraud, service accounts, sell products and services to customers and third parties, perform marketing, hire and manage our employees, comply with legal and regulatory obligations, improve the quality of our services, respond to customer complaints, assert and defend legal claims, and to secure our assets and those of our customers.

We comply with lawful requests for information from law enforcement, regulators, judicial authorities and court-appointed trustees, supervisors, and other third parties pursuant to subpoenas or document requests. Therefore, we may share your information with authorized issuers, processors, or facilitators of subpoenas, summons, search warrants, levies, garnishments and similar legal process.

We may also disclose your information to a third party to enforce our agreements and policies, to protect the security or integrity of the Bank, its services and assets, to protect customers or the public from harm or illegal activities, to respond to an emergency which we believe reasonably requires us to disclose information to assist in preventing death or serious bodily injury, or, with your prior consent, to any other third party.

More specific categories and uses:

- A. If you are an authorized user of a business deposit account, we collect your identifying information, and potentially biometric information, from any account documentation and from the account opening process. We also collect information regarding transactions related to the business deposit account. This information may be used to make credit decisions, secure your information, prevent fraud, service accounts, analyze network traffic, comply with legal and regulatory obligations, and for marketing purposes.
- B. If you are or seek to be a lessee, borrower or guarantor on a credit agreement for a business purpose loan, lease, or other credit product, we collect your identifying information and financial information, such as tax returns and financial statements, some of which may include protected classifications, geolocation and network activity information, commercial information, and/or professional or employment-related information. For certain types of loans we may also be required to collect these categories of personal information related to your employees. This information is obtained from both the financial information provided to the Bank during the loan application process, as well as any subsequent follow up inquiries. This information is used to make credit decisions, secure your information, prevent fraud, service accounts, analyze network traffic, comply with legal and regulatory obligations, and for marketing purposes.
- C. We collect identifying information about trust settlors, trustees, and beneficiaries to make credit decisions, secure loans, provide trust-related services, secure your information, prevent fraud, comply with legal and regulatory obligations, and for marketing purposes.
- D. We collect identifying information and financial information about individuals involved in establishing, facilitating and/or engaging in deposit account activities, including ACH Direct Deposit information. This information is used to make credit and deposit decisions, secure your information, prevent fraud, service accounts, comply with legal and regulatory obligations, and for marketing purposes.

- E. We collect identifying information about individuals or entities with which our customers do business to complete transactions, make credit decisions, service accounts, originate loans, comply with legal and regulatory obligations, secure your information, and prevent fraud.
- F. We collect audio, biometric (voiceprint), and network activity information regarding calls on recorded lines, which may or may not include other personal information. This information is used to authenticate individuals, confirm orders, resolve disputes, respond to credit requests, secure your information, prevent fraud, service accounts, comply with legal and regulatory obligations, and for marketing purposes.
- G. We collect video at our ATMs at the time that transactions occur, and inside our branches and offices. This information is used for security, to resolve disputes, comply with legal and regulatory obligations, and to prevent fraud.
- H. We collect personal information contained in communications transmitted using Bank-owned devices and equipment, or on personally owned devices or equipment which operate Bank-owned or licensed applications, to secure the bank and its assets, prevent fraud, service accounts, and comply with legal and regulatory obligations.
- I. We may collect health screening information and/or COVID-19 vaccine information about individuals who enter our offices or branches where required to comply with applicable laws and regulations.
- J. We collect identifying information about business contacts at vendors, service providers, bank counterparties, and other business partners, some of which may be protected class information, where reasonably necessary for the Bank's operations, to comply with legal and regulatory obligations, secure your information, and to prevent fraud.
- K. We collect personal information about business contacts at non-profit and charitable organizations with which the Bank works or to which the Bank provides services. This information is used to assist in the Bank's charitable, redevelopment, and philanthropic efforts, make credit decisions, prevent fraud, service accounts, open new deposit accounts, to comply with legal and regulatory obligations, and for marketing purposes.
- L. We collect identifying information about business contacts at affiliates to further the Bank's business activities and interests, to comply with legal and regulatory obligations, to prevent fraud, and where reasonably necessary for the Bank's operations.
- M. We collect identifying information about business contacts at various regulatory entities, legal firms, and trade organizations for purposes of complying with applicable laws, employee training and education, lobbying, cooperative projects, and seeking legal and/or consulting advice.

- N. We collect personal information about current, past, and prospective employees of the Bank and their dependents, including individual identifier information, protected class information, commercial, network activity, audio, video, electronic, visual, professional, employment-related, and education information, for general business purposes, physical security, information security, business continuity, hiring, employment, vetting, payroll, employment benefit, public relations, analytics and other employment-related purposes, to comply with legal and regulatory obligations, risk management, and to prevent fraud. For a small subset of employees we collect fingerprint information for physical security purposes. For most employees, we collect a photo for identification and security purposes. We may collect additional personal information for employees that elect to make use of a company credit card, or who volunteer additional emergency contact or other information. We may collect health screening information about our employees, including thermal (body temperature) and olfactory (sense of smell) information, for the protection of our employees and customers from COVID-19 and other contagious illnesses. We may collect COVID-19 vaccine information about employees where required to comply with applicable laws and regulations.
- O. We collect identifying, professional, employment, educational, and consumer profile information about customer prospects and leads for marketing and statistical purposes, to respond to questions and complaints, and to comply with legal and regulatory obligations.
- P. We collect identifying information and network activity information from visitors to our online and mobile websites and users of our mobile applications to deliver services, remember users and their preferences, perform statistical analysis, authenticate users, comply with legal and regulatory obligations, prevent fraud, detect and respond to security incidents, for marketing purposes, and to deliver information to prospective and current online account holders, as further described in our [Online Privacy Notice](#).
- Q. We collect identifying information about individuals, business contacts, entity trust settlors and trustees for the purpose of entering into commercial landlord/tenant relationships.

Bank of the West collects personal information directly from consumers and other individuals, and from other sources, including the following:

- A. Credit bureaus;
- B. State and federal bureaus, agencies, and departments;
- C. Public websites and social media;
- D. Vendors and service providers;
- E. Other financial institutions;

- F. Transactional counterparties;
- G. Employee and customer referrals; and
- H. Affiliates.

Bank of the West discloses the following categories of personal information:

- A. We disclose employee and employee dependent identifying information, professional information, and/or protected classification information to vendors who contract with the Bank to provide services and benefits to employees and the Bank, to legal and regulatory agencies, to affiliates, to third parties in connection with a proposed or actual sale or merger, and to third party lenders. We disclose employee contact information where reasonably necessary for the Bank's operations, to secure the Bank's employees and assets, for employee career development, to prevent fraud, seek legal advice, respond to court orders, investigations and regulatory inquiries, and comply with legal and regulatory obligations. We disclose employee health screening information to governmental agencies, departments, and healthcare providers as required to comply with applicable laws and regulations, for the protection of our employees and customers, and where necessary to facilitate employee health benefits. We may disclose COVID-19 vaccine information about employees where required to comply with applicable laws and regulations.
- B. We disclose personal information about prospective employees, including individual identifier information, protected class information, commercial, network activity, professional, and/or education information to third party vendors and affiliates who contract with the Bank to assist with background checks, candidate search, onboarding, to prevent fraud, seek legal advice, and to respond to court orders, regulatory inquiries, and legal investigations, respond to questions, and complaints and otherwise where reasonably necessary for the Bank's operations.
- C. We disclose the personal information of our current and prospective commercial customer contacts and associated individuals, which may include individual identifier information, protected class information, commercial, biometric, network activity, financial, and/or professional information to third party vendors, credit bureaus, state and federal bureaus, agencies, and departments, transactional counterparties, and other financial institutions and affiliates to service accounts, conduct background and credit checks, facilitate transactions, for marketing purposes, to prevent fraud, money laundering or terrorist financing, seek legal advice, and to respond to court orders, regulatory inquiries, and legal investigations, and otherwise where reasonably necessary for the Bank's operations.