



California Consumer Privacy Policy

Last Updated: September 1, 2026

Mission Valley Bank ("MVB," "the Bank," "we," "our," or "us") is committed to protecting personal information. This California Consumer Privacy Policy ("Policy") applies to California residents only ("consumers" or "you") and explains our practices under the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 (collectively, the "CCPA"). Terms defined by the CCPA have the same meanings when used in this Policy.

Certain personal information is exempt from, or outside the scope of, the CCPA. For example, certain information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act and its implementing regulations is not subject to the CCPA. Other exemptions may also apply depending on the information and context.

1. Definitions

The following are definitions of terms that you will see in this Policy.

- **"We", "our", and "us"** refer to Mission Valley Bank.
- **"You" and "your"** refer to a **natural person who is a California resident**.
- **"Personal Information"** is information that identifies, relates to, or could reasonably be linked directly or indirectly with a particular individual or household.
- **"Categories of Personal Information" and "Categories of Sensitive Personal Information"** - Unless otherwise specified, references in this Notice to "Personal Information" include both Personal Information and Sensitive Personal Information as defined under the CCPA.

2. Personal Information We Collect

During the preceding 12 months, we have collected the following categories of personal information and categories of sensitive personal information, depending on the consumer's relationship and interactions with the Bank:

- **"Categories of Personal Information"** are as follows:
 - **Identifying Information** is information that identifies an individual, such as an individual's name, alias, birthdate, account name or other similar identifiers.
 - **Associated Information** is information that relates to, describes, or can reasonably be associated with a particular individual such as a signature, postal or email address, telephone number, insurance policy number, bank account or card number, and any similar information.
 - **Characteristic Information** is information related to characteristics of protected classifications under state or federal law, such as gender or marital status or beneficiary information.
 - **Commercial Information** is information of a commercial nature, such as records of personal property, products or services purchased or considered, or other purchasing histories.
 - **Biometric Information** is information related to the measurement or analysis of unique physical or behavioral characteristics, such as a fingerprint or voice pattern.
 - **Geolocation Information** is information or data related to a geographical location, such as a device or Internet Protocol (IP) location.
 - **Audio, Electronic, Visual Information** includes security camera recordings from Bank facilities, telephone call recordings, meeting recordings, and other audio, visual, electronic, or similar information collected in connection with the Bank's operations.
 - **Internet Activity Information** is information related to internet or other electronic network activity, such as a search or browsing history, interactions with our website or online services, device information and related website analytics information.
 - **Financial Information** is information related to bank accounts held with us or other financial institutions such as your bank account number, or debit or other payment card information.



- **Employment Information** is professional or employment-related information, such as employment history or status.
- **Inference Information** is inferences drawn from any other category of personal information to create a profile about an individual reflecting potential or probable preferences, behavior, abilities, or other similar predispositions.
- **“Categories of Sensitive Personal Information”** are as follows:
 - **Identification Numbers** are any information that reveals an individual’s social security number, driver’s license number, state identification card number, or passport number.
 - **Financial Account Credentials** are any information that reveals an individual’s account log-in number, financial account number (such as a loan number or deposit account number), debit card number, or credit card number in combination with any required security or access code, password, or credentials which would allow someone to gain access to the account.
 - **Background Information** is any information that reveals an individual’s racial or ethnic origin.
 - **Personal Messages** are the contents of an individual’s mail, email, and text messages if the individual is an employee of the Bank, and where the Bank is not the intended recipient of the communication.
 - **Health Information** is any personal information collected and analyzed concerning an individual’s health.

3. Sources of Personal Information

We collected the Personal Information from the following sources:

- You directly, including through applications, forms, communications, and transactions.
- Corporate customers and other organizations that provide information about individuals associated with them, such as owners, officers, employees, guarantors, or board members.
- Service providers, vendors, and other parties that support our operations.
- Credit reporting agencies and other information providers.
- Commercial data providers and public or government sources.
- Employers, educational institutions, and outside companies used to support Human Resources and workforce-management activities.
- Persons and entities involved in transactions with you.
- Our branches, security systems, websites, cookies, and website analytics technologies.

4. Purposes for Collecting and Using Personal Information

In the past 12 months, we collected the Personal Information about consumers for the following business or commercial purposes:

- **Operational** – Providing services to the Bank, our customers, employees, applicants, and other authorized parties, including maintaining and servicing accounts; processing transactions and payments; providing customer service; verifying identity and customer information; processing employment applications; administering employee benefits and compensation; and carrying out other day-to-day business operations.
- **Operational purposes** also include validating identity when an individual accesses or uses our websites, applications, products, services, branches, or other customer service channels.
- **Website Operations and Security** – Operating, maintaining, securing, measuring, and improving our websites, applications, and online banking services, mobile banking services and other online services, including through basic website analytics and performance-monitoring technologies.
- **Marketing** – Marketing the Bank’s products and services and identifying prospective customers. The Bank does not use Sensitive Personal Information for advertising or marketing purposes.



- **Commercial** – Activities that advance our commercial or economic interests (e.g., activities that induce customers to obtain or maintain products and services with us) or that enable or effect transactions. Identify and contact prospective commercial customers and market the Bank's products and services, including through information obtained from commercial data providers.
- **Security** – Activities to protect against malicious, deceptive, fraudulent, or illegal activity, detect security incidents, or hold the perpetrators of that activity responsible.
- **Compliance** – Activities to achieve, verify, or maintain compliance with our policies and procedures or applicable legal and regulatory standards and obligations.
- **Audit** – Auditing compliance with our policies and procedures or applicable legal and regulatory standards and obligations.

5. Disclosure of Personal Information

The categories of third parties to whom we disclosed Personal Information for our business purposes described in this privacy policy are:

- Vendors and service providers, including information technology, infrastructure, cybersecurity, website analytics, mailing, email delivery, document management, and auditing providers.
- Financial, payment, communications, storage, legal, tax, notary, and professional service providers.
- Marketing service providers that assist the Bank in communicating with customers or prospective commercial customers, subject to applicable contractual and legal requirements.
- Government agencies, regulators, law enforcement, courts, and other parties as required or permitted by law.
- Consumer reporting agencies and other outside companies used for routine or legally required reporting.
- Employment and benefits providers.
- Third parties that provide or support online banking, mobile banking, account opening, payment processing, digital communication, and other electronic banking services.
- Other parties at your direction or with your authorization.
- Other parties as required or permitted by law.

6. Sale or Sharing of Personal Information

We do not sell personal information for monetary or other valuable consideration, and we do not share personal information for cross-context behavioral advertising, as those terms are defined by the CCPA. During the preceding 12 months, we have not sold or shared personal information, including personal information of consumers under 16 years of age.

Because we do not sell or share personal information as defined by the CCPA, we do not provide a "Do Not Sell or Share My Personal Information" link. We nevertheless periodically review our website technologies, commercial data practices, and marketing arrangements to confirm that this statement remains accurate. If our practices change, we will update this Policy and implement applicable consumer choice mechanisms.

7. Use and Disclosure of Sensitive Personal Information

We use and disclose sensitive personal information only for purposes permitted by the CCPA and its implementing regulations. We do not use or disclose sensitive personal information for purposes that trigger the right to limit its use or disclosure.



8. Your California Privacy Rights

Right to Know and Access

You have the right to know and request what personal information we have collected about you, including categories and specific pieces of personal information, categories of sources, purposes for collection and use, and categories of recipients.

Right to Delete

You may request deletion of personal information that we collected from you, subject to applicable exceptions.

Right to Correct

You may request correction of inaccurate personal information that we maintain about you. We will consider the nature of the information and the purpose for which we maintain it when responding to a correction request.

Right to Non-Discrimination

You have the right not to receive discriminatory treatment for exercising rights provided by the CCPA. Employees, applicants, and independent contractors also have the right not to be retaliated against for exercising applicable CCPA rights.

9. How to Submit a Request

You may submit a request to know, access, delete, or correct through any of the following methods:

- **Telephone:** (877) 685-9265
- **Email:** compliance@missionvalleybank.com
- **Mail:** Mission Valley Bank, Attention: Compliance Department, 2777 N. Ontario Street, Suite 130, Burbank, CA 91504

We will use a reasonable verification process that considers the nature and sensitivity of the personal information involved. We may request information necessary to match you to our records and protect against fraudulent requests. If we cannot verify a request, we will explain the basis for the denial or limitation, as applicable.

10. Authorized Agents

You may authorize an agent to submit a request on your behalf. We may require proof that the agent has permission to act for you and may require you to verify your identity directly with us, unless applicable law provides otherwise. Authorized-agent requests may be submitted using the contact methods listed above.

11. Response Timing

We will confirm receipt and respond to verifiable requests within the timeframes required by applicable law. We generally respond to requests to know, delete, or correct within 45 days after receipt. When reasonably necessary, we may extend the response period once by an additional 45 days and will notify you of the extension and the reason for it within the initial 45-day period.

12. Data Retention

We retain personal information only for as long as reasonably necessary and proportionate to achieve the purposes described in this Policy, comply with legal and regulatory requirements, resolve disputes, enforce agreements, and respond to audits, investigations, litigation, or other legal matters. Retention periods vary based on the nature of the information, the purpose for which it is maintained, and applicable record-retention requirements.



13. Changes to This Policy

We may update this Policy to reflect changes in our practices, legal requirements, or regulatory guidance. The “Last Updated” date at the beginning of this Policy identifies the most recent revision. Material changes will be communicated as required by applicable law.

14. Contact Us

For questions or concerns about this Policy or our privacy practices, contact:

Mission Valley Bank

Attention: Compliance Department

2777 N. Ontario Street, Suite 130

Burbank, CA 91504

Email: compliance@missionvalleybank.com

Telephone: (877) 685-9265