



Notice at Collection – California Consumer Privacy Notice California Consumer Privacy Act (“CCPA”)

Scope and Overview

This Notice at Collection – California Consumer Privacy Notice (“**Consumer Privacy Notice**”) supplements the information contained in PCB Bank’s [California Privacy Notice](http://www.mypcbbank.com/privacy-policy/privacy-notice-for-california-residents) (see www.mypcbbank.com/privacy-policy/privacy-notice-for-california-residents) and applies to all consumers who reside in the State of California ("consumers" or "you"). We adopt this notice to comply with the California Consumer Privacy Act of 2018 (**CCPA**) and any terms defined in the **CCPA** have the same meaning when used in this **Notice**.

PCB Bank is committed to protecting the privacy and security of your personal data. This Notice at Collection - **Consumer Privacy Notice** describes how PCB Bank and its subsidiaries, affiliates, and related entities (collectively, "PCB Bank," "PCB," "we," or "us") collect and process personal data about you prior to, during, and after the period in which you receive products and services from us. This **Consumer Privacy Notice** applies to individuals who are residents of California.

This **Consumer Privacy Notice** describes the categories of personal data that we collect, how we use your personal data, how we secure your personal data, when we may disclose your personal data to third parties, *and* when we may transfer your personal data outside of California. This **Consumer Privacy Notice** also describes your rights regarding the personal data that we hold about you including how you can access, correct, and request erasure of your personal data.

We will only process your personal data in accordance with this **Consumer Privacy Notice** unless otherwise required by applicable law. We take steps to ensure that the personal data that we collect about you is adequate, relevant, not excessive, and processed for limited purposes.

Collection of Personal Data

For purposes of this **Consumer Privacy Notice**, personal data means any information about an identifiable individual. Personal data **excludes** anonymous or de-identified data that is not associated with a particular individual, publicly available information from government records, and information excluded from the CCPA’s scope, such as personal information covered by certain sector-specific laws, including the Fair Credit Reporting Act (“FCRA”), the Gramm-Leach-Bliley Act (“GLBA”) or California Financial Information Privacy Act (“CFIPA”), the Driver’s Privacy Protection Act of 1994, among other exemptions. To carry out our activities and obligations as your banking institution, we may collect, store, and process the following categories of personal data for the purpose of managing and servicing our banking relationship with you:

Identifiers

- Personal contact details such as nickname or alias, DBA or company/brand name, legal name, title, present and former addresses, length of residence, telephone numbers, personal email addresses.
- Identifiers such as your account name and number, signature, debit card number, Internet Protocol address, customer login device, user identification, password, physical characteristics or description, or similar identifiers.
- Government identification numbers such as a taxpayer identification number, passport number, driver's license number or state identification number, or other identification card number.

Personal, Employment, and Commercial Information

- Date of birth.

- Marital and dependent status. Spousal information may be collected in accordance with state and federal law, including the intent to apply for joint credit.
- Account signers, account beneficiaries, power-of-attorney, or other account relationships, and name of nearest relative not living with you.
- Business/corporate legal documentation, ownership and shareholders, ownership history, business licenses, officers, employees, and management succession. Customers, suppliers, or other vendors.
- Financial information regarding your assets such as financial statements, detailed bank or investment account and IRA/401K information including documentation of your transaction history, source of down payment, income, source of wealth, profit or loss, sales, accounts receivable, rental income and terms, tenants accounts payable, personal property, fixtures equipment, inventory, real estate owned including occupancy status, sales agreements, pricing, or any other information about your financial condition that may include detailed and proprietary information on products and services offered to your customers. For deposit accounts at PCB, we will also inquire about normal and expected account activity, and online gambling services.
- Financial information regarding your liabilities including: financial statements, profit or loss, credit card or loan statements, credit history, type of loan and loan purpose, payment history, purchase agreements, loan collateral, guarantors, lease payments or similar obligations and terms, other debt or loan information, co-signer or co-maker on a loan, alimony or child support payments, court records, information regarding delinquent obligations, repossession, deed-in-lieu, or foreclosure, bankruptcy; claims, lawsuits, or legal actions, or any other information about your financial condition that may include detailed and proprietary information on products and services offered to your customers.
- Records of personal property or real estate, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
- Service agreements with other third parties including asset or property management, mortgage brokers.
- Tax records including unpaid taxes.
- Title searches, property vesting, and transfers of ownership for real property.
- Property appraisals, flood zone determination and maps, environmental hazards.
- Subpoenas, liens, and law enforcement requests in accordance with applicable law
- Payor or payee information including the depository institution name, routing number, and branch.
- Information required by the Small Business Administration (SBA) regarding prior loan experience, any prior SBA loan losses, detailed product and service information, federal government transaction eligibility, and whether you are a government official, government employee, Small Business Advisory member, or SCORE volunteer.
- Personal references, financial institution references, background and internet searches, and referral source information.
- Insurance information including policy number and details of insurance coverage including the policy.
- Current or past employment history and corresponding information such as start date, job title and duties, employer address, telephone number, and income verification.
- Education, training, or licenses.
- Photograph for identification purposes.

Biometric Information

- Genetic, physiological, behavioral, and biological characteristics, or activity patterns used to extract a template or other identifier or identifying information, such as, fingerprints, keystrokes, face prints, and voiceprints, video records, telephone recordings, iris or retinal scans, gait, or other physical patterns, and sleep, health, or exercise data.

Internet

- Browsing history, search history, information on a consumer's interaction with a website, application, or advertisement.

Geolocation Data

- Physical location or movements.

Protected Classifications

- Protected classification characteristics under California or Federal law including age, ethnicity, race, color, ancestry, national origin, birthplace, citizenship, immigration status, religion or creed, marital status, medical condition, physical or mental disability, sex, familial status, veteran or military status.

Sensory

- Audio, electronic, visual, thermal, olfactory, or similar information.

Inferences Drawn

- Profile reflecting a person's preferences, characteristics, psychological trends, predispositions, behavior, criminal records, attitudes, intelligence, abilities, and aptitudes.
- Other personal details that you otherwise voluntarily provide to us.

We will collect the majority of the personal data that we process directly from you. In limited circumstances third parties may provide your personal data to us, such as current or former employer(s), credit reporting agencies, official bodies (such as regulators or criminal record bureaus), or other applicable sources related to your transactions or accounts with us.

Use of Personal Data

We only process your personal data where applicable law permits or requires it, including where the processing is necessary for providing banking products and services to you, where the processing is necessary to comply with a legal obligation that applies to us, for our legitimate interests or the legitimate interests of third parties, to protect your vital interests, or with your consent if applicable law requires consent. We may process your personal data for the following legitimate business purposes and for any other purposes of providing banking products and services to you:

- To fulfill or meet the reason you provided the information. For example, if you share your name and contact information to ask a question about our products or services, we will use that personal information to respond to your inquiry. If you provide your personal information to purchase a product or service, we will use that information to process your payment and facilitate delivery.
- To provide, support, personalize, and develop our Website, products, and services.
- To create, maintain, customize, and secure your account with us.
- To process your requests, purchases, transactions, and payments and prevent transactional fraud.
- To carry out our obligations and enforce rights arising from any contracts entered into between you and us, including for billing and collections.
- To provide you with support and to respond to your inquiries, including to investigate and address your concerns and monitor and improve our responses.
- To help maintain the safety, security, and integrity of our Website, products and services, databases and other technology assets, and business.
- For testing, research, analysis, and product development, including to develop and improve our Website, products, and services.
- Accounting and auditing, including examinations by banking regulatory agencies.
- To respond to law enforcement requests and to comply with our legal, regulatory, or other corporate governance requirements.
- As described to you when collecting your personal information or as otherwise set forth in the **CCPA**.
- To evaluate or conduct a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of our assets, whether as a going concern or as part of bankruptcy, liquidation, or similar proceeding, in which personal information held by us about our consumers is among the assets transferred.

We will only process your personal data for the purposes we collected it for or for compatible purposes. If we need to process your personal data for an incompatible purpose, we will provide **notice** to you and, if required by law, seek your consent. We may process your personal data without your knowledge or consent only where required by applicable law or regulation.

We may also process your personal data for our own legitimate interests, including, but not limited to, the following purposes:

- To prevent fraud.
- To ensure network and information security, including preventing unauthorized access to our computer and electronic communications systems and preventing malicious software distribution.

The above listed items in the “Collection of Personal Data” and the “Use of Personal Data” do not represent an exhaustive list, and PCB reserves the right to amend the list at any time as we continue to develop our compliance program in response to further legal developments and new interpretations of the CCPA.

Collection and Use of Special Categories of Personal Data

Bank collects sensitive personal information. Sensitive Personal Information is defined as follows:

Personal information that reveals:

- (A) A consumer’s social security, driver’s license, state identification card, or passport number.
- (B) A consumer’s account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account.

The following special categories of personal data, if collected, may be considered sensitive and may receive special protection:

- Racial or ethnic origin.
- Citizenship or immigration status
- Political opinions.
- Religious or philosophical beliefs.
- Trade union membership.
- Biometric data.
- Data regarding payments for health services.
- Data relating to criminal convictions and offences.

We may collect and process the following special categories of personal data when you voluntarily provide them for the following legitimate business purposes, to carry out our obligations under applicable laws and regulations, for providing banking products and services, or as applicable law otherwise permits:

- Race or ethnic origin for government reporting purposes.

Where we have a legitimate need to process special categories of personal data about you for purposes not identified above, we will only do so only after providing you with **notice** and, if required by law, obtaining your prior, express consent.

Data Sharing

We will only disclose your personal data to third parties where required by law or to our employees, contractors, designated agents, or third-party service providers who require such information to assist us with providing banking products and services to you, including third-party service providers who provide services to us or on our behalf. Third-party service providers may include, but are not limited to, data storage or hosting providers. These third-party service providers may be located outside of California.

We require all our third-party service providers, by written contract, to implement appropriate security measures to protect your personal data consistent with our policies and any data security obligations applicable to us as your banking products and services provider. We do not permit our third-party service providers to process your personal data for their own purposes. We only permit them to process your personal data to the limited extent required to provide their services to us, and only to carry out the purpose for which we disclosed your personal data to them. Third-party service providers are not

permitted to use your personal data for any other purpose or in any manner that would constitute a violation of any federal, state or local financial and/or banking laws or regulations including, but not limited to, the California Consumer Privacy Act and the Gramm-Leach-Bliley Act.

We may also disclose your personal data for the following additional purposes where permitted or required by applicable law:

- To our affiliates, including PCB Bancorp, for the purposes set out in this **Consumer Privacy Notice** and as necessary to provide banking products and services to you.
- As part of our regular reporting activities to our affiliates, including PCB Bancorp.
- To comply with legal obligations or valid legal processes such as search warrants, subpoenas, or court orders. When we disclose your personal data to comply with a legal obligation or legal process, we will take reasonable steps to ensure that we only disclose the minimum personal data necessary for the specific purpose and circumstances.
- To protect the rights and property of PCB Bank and its affiliates, including PCB Bancorp.
- During emergency situations or where necessary to protect the safety of persons.
- Where the personal data is publicly available.
- If a business transfer or change in ownership occurs and the disclosure is necessary to complete the transaction. In these circumstances, we will limit data sharing to what is necessary, and we will anonymize the data where technically and reasonably feasible.
- For additional purposes with your consent where such consent is required by law.

Data Security

We have implemented appropriate physical, technical, and organizational security measures designed to secure your personal data against accidental loss and unauthorized access, use, alteration, or disclosure. In addition, we limit access to personal data to those employees, agents, contractors, and other third parties that have a legitimate business need for such access.

Data Retention

Except as otherwise permitted or required by applicable law or regulation, we will only retain your personal data for as long as necessary to fulfill the purposes we collected it for, as required to satisfy any banking laws and regulations governed by various regulatory agencies, legal, accounting, or reporting obligations, or as necessary to resolve disputes. To determine the appropriate retention period for personal data, we consider our statutory obligations, the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorized use or disclosure of your personal data, the purposes we process your personal data for, and whether we can achieve those purposes through other means. We specify the retention periods for your personal data in our data retention policy.

Under some circumstances we may anonymize your personal data so that it can no longer be associated with you. We reserve the right to use such anonymous and de-identified data for any legitimate business purpose without further **notice** to you or your consent. We will retain and securely destroy your personal data in accordance with our document retention policy and applicable laws and regulations based upon the nature of the products and services you obtained from us.

Rights to Know, Right to Correct and Right to Delete

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes. By law, you may have the right to request access to, correct, and delete the personal data that we hold about you, subject to all retention laws under the applicable banking laws and regulations governed by various banking regulatory agencies.

We may request specific information from you to confirm your identity in order to process your right to access, correct and delete your personal data. Applicable law may allow or require us to refuse to provide you with access to some or all of the personal data that we hold about you, or we may have destroyed, deleted, or made your personal data anonymous in

accordance with our record retention obligations and practices. If we cannot comply with your request, we will inform you of the reasons why, subject to any legal or regulatory restrictions.

Exercising Access, Data Portability, Correction and Deletion Rights

To exercise the access, data portability, correction and deletion rights described above, please submit a verifiable consumer request to us by either:

- Calling us at (888) 979-8133.
- Emailing us at privacy@mypcbbank.com
- Visiting www.mypcbbank.com/privacy-policy
- Completing a written form at any of our PCB Bank locations

Only you, or someone legally authorized to act on your behalf, may make a verifiable consumer request related to your personal information. You may also make a verifiable consumer request on behalf of your minor child. To designate an authorized agent, please complete the Right to Know and Right to Delete Request form, or Right to Correct Form include the contact information in the space provided, and sign and date the form. We cannot respond to your request if we cannot verify your identity or if we do not receive proper document supporting/evidencing authorization to make request on your behalf.

We will only use personal information provided in a verifiable consumer request to verify the requestor's identity or authority to make the request. You may only make a verifiable consumer request for access or data portability twice within a 12-month period. Making a verifiable consumer request does not require you to create an account with us.

Right to Opt-Out

We do not sell the personal information of consumers, and minors we actually know are less than 16 years of age. Therefore, it is not necessary to opt-out.

Changes to This Consumer Privacy Notice

We reserve the right to update this **Consumer Privacy Notice** at any time, and we will provide you with a new **Consumer Privacy Notice** when we make any updates. If we would like to use your previously collected personal data for different purposes than those we notified you about at the time of collection, we will provide you with **notice** and, where required by law, seek your consent, before using your personal data for a new or unrelated purpose.

Contact Information

If you have any questions or comments about this notice, the ways in which PCB Bank collects and uses your information described below and in the [California Privacy Policy](#), your choices and rights regarding such use, or wish to exercise your rights under California law, please do not hesitate to contact us at:

Phone: (888) 979-8133

Website: www.mypcbbank.com/privacy-policy

Email: privacy@mypcbbank.com

Postal Address:

PCB Bank
Attn: Compliance Department
3701 Wilshire Boulevard, Suite 900
Los Angeles, California 90010