

**PLAINS COMMERCE BANK**

**CALIFORNIA PERSONNEL PRIVACY POLICY**

**TABLE OF CONTENTS**

[I. PURPOSE 2](#_Toc206757725)

[II. POLICY STATEMENT 2](#_Toc206757726)

[California Notice at Collection 2](#_Toc206757727)

[Personal Information We Collect 2](#_Toc206757728)

[Sources of Personal Information 3](#_Toc206757729)

[Uses of Personal Information 3](#_Toc206757730)

[Personal Information Disclosures 4](#_Toc206757731)

[Personal Information Sales or Sharing 5](#_Toc206757732)

[Privacy Rights 5](#_Toc206757733)

[Personal Information Retention 5](#_Toc206757734)

[Contact Information 5](#_Toc206757735)

# PURPOSE

Plains Commerce Bank (Bank), its subsidiaries, affiliates, successors, assigns, or any third parties acting on the Bank’s behalf provides you with this California Personnel Privacy Policy (Policy) describing the Bank’s privacy practices relating to the personal information that the Bank will collect, use, and disclose about candidates for employment, applicants for employment, employees, independent contractors, contractor employees, temporary workers, volunteers, apprentices, owners, directors, officers, and other individuals engaged by the Bank or acting on the Bank’s behalf (personnel, you, your), who are residents of California and subject to the California Consumer Privacy Act (CCPA).

This Policy is directed at Bank personnel, who may also be customers. Please refer to the Privacy Policy posted to the Bank’s website ([www.plainscommerce.com](http://www.plainscommerce.com)) for more information about the Bank’s handling of your personal information as a customer.

# POLICY STATEMENT

## California Notice at Collection

The Bank collects the categories of personal information as described under the “Personal Information We Collect” section below. The Bank uses these categories of personal information for the purposes as described under the “Uses of Personal Information” section below, and the Bank discloses it as described under the “Personal Information Disclosures” section below. The Bank retains your personal information as described under the “Personal Information Retention” section below.

## Personal Information We Collect

Personal information identifies, relates to, describes or is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly to a particular individual or household. The Bank may have collected the following categories of personal information about the Bank’s personnel within the last twelve (12) months:

* Identifiers, such as name, contact information, online identifiers, government-issued identifier, and other unique identifiers (e.g., employee ID).
* Personal information, such as first and last name, signature, physical characteristics or description, address, telephone number, passport number, driver’s license or state identification card number, passport number, federal identification authorizing work in the United States, access and/or passcodes, insurance policy number, education, employment, employment history, bank account number, other financial information, medical information, or health insurance information.
* Protected classification characteristics under California or federal law, such as age, marital status, gender, sex, race, color, disability, citizenship, primary language, immigration status, military/veteran status, disability, request for leave, and medical conditions.
* Commercial information, such as transaction information and purchase history (e.g., in connection with travel or other reimbursements).
* Internet or network activity information, such as browsing history and interactions with Bank online systems and websites and any personal information that you provide while accessing the Bank’s computer systems, such as personal credit card information and passwords.
* Geolocation data, such as device location from usage of the Bank’s devices.
* Biometric information, such as facial recognition and fingerprints related to access to the Bank’s secured access points.
* Audio, electronic, visual, and similar information, such as images and audio, video, or call recordings created in connection with Bank business activities.
* Professional or employment-related information, such as work history and prior employer, human resources data, and data necessary for benefits and related administrative services.
* Education information, subject to the federal Family Educational Rights and Privacy Act, such as student records.
* Inferences drawn from any of the personal information listed above to create a profile or summary about you, for example, your preferences, abilities, aptitudes, and characteristics.
* Sensitive personal information, such as your Social Security number, driver’s license, state identification card, or passport number; account log-in or credentials allowing access to an account; precise geolocation; racial or ethnic origin, citizenship or immigration status, religious or philosophical beliefs, or union membership; the contents of mail, email, and text messages; genetic data; neural data; biometric information; health information; or sex life or sexual orientation.
* Commercial information, including records of personal property; products or services purchased, obtained, or considered; or other purchasing or consuming histories or tendencies.
* Any other personal information the Bank may collect with your consent or for other legitimate business purposes to manage the Ban’s personnel. For example, the Bank may ask you to participate in surveys, contests, or other voluntary personnel programs that may ask you to provide personal information.

The Bank may collect certain personal information automatically through your use of Bank information technology systems, devices, networks, and electronic communication tools, such as your Internet protocol (IP) address, inferred location based on your IP address or activities, device identifiers associated with your computer or device, mobile carrier and related information, activity logs, and other information about activities you engage in on Bank property, equipment, accounts, systems and networks. The Bank may monitor and review uses of Bank equipment, accounts, information technology systems and networks, including its phone networks, computer networks, including those used to access the Internet, videoconferencing systems and other Bank-provided electronic communications tools. The Bank may access and review electronic files, messages, and emails sent or stored on its information technology systems, including accounts, computers and devices provided to personnel. For avoidance of doubt, this Policy does not establish, and should not be construed to mean, that all personnel will have access to, or will participate in, the systems, networks, data, programs and other business activities described in this Policy.

Personal information does not include:

* Publicly available information from government records, or lawfully obtained, truthful information that is a matter of public concern.
* De-identified or aggregated information.

## Sources of Personal Information

The Bank may collect the above-mentioned categories of personal information about you from the following sources: 1) you; 2) internally generated information, such as human resources, vendor management, or other administrative teams; 3) prior employers, employment agencies, recruiters, references, or job-related social media platforms; 4) service providers, such as benefits and payroll administrators; and 5) other third-party sources, such as consumer reporting agencies, background check providers, drug testing facilities, advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and data brokers.

## Uses of Personal Information

The Bank may use your personal information for any of the following commercial or business purposes:

* To operate, manage, and maintain Bank business.
* For hiring, retention, and human resources purposes, for example to:
	+ Communicate with you about your engagement with the Bank, including providing training, Information Technology (IT) support, and other relevant interactions.
	+ Evaluate job applicants and candidates for employment.
	+ Assess your suitability, aptitude, skills, qualifications, and interests for job responsibilities.
	+ Obtain and verify background checks.
	+ Assist you with obtaining an immigration visa or work permit (where required and requested by you).
	+ Grant and monitor employees’ access to secure Bank facilities.
	+ Provide you with information about employee benefits, training, or opportunities of interest to you.
	+ Workflow management, including assigning, managing, and administering projects as well as to track time and attendance.
	+ Processing payroll and compensation, including bonuses and long-term incentive administration, stock plan administration, compensation analysis, including monitoring overtime and compliance with labor laws, and Bank recognition programs.
	+ Administer and maintain benefits, including group health insurance and retirement service.
	+ Process workers’ compensation claims.
	+ Manage employee performance of their job duties, including promotions, discipline, and/or termination.
	+ Conduct workplace investigations.
	+ Take disciplinary action, address injuries, and resolve other workplace related incidents.
	+ Verifying compliance with any contractual obligations.
	+ Fulfill any other reasons for which the personal information is collected.
* To otherwise accomplish the Bank’s legitimate business purposes and objectives, including, for example:
	+ Implement, monitor, and manage electronic security measures on devices that are used to access networks and systems (e.g., incident management).
	+ Engage in corporate transactions requiring review of employee records, such as for evaluating potential mergers and acquisitions of the Bank.
	+ Maintain commercial insurance policies and coverages, including for workers’ compensation and other liability insurance.
	+ Anonymize and/or aggregate data to perform workforce analytics, data analytics, and benchmarking.
	+ Perform call monitoring and surveillance.
	+ Provide, validate, or communicate services offered to Bank personnel.
	+ Emergency services.
	+ Conducting research, analytics, and data analysis.
	+ Maintaining Bank facilities and infrastructure.
	+ Quality and safety assurance measures.
	+ Conducting risk and security controls and monitoring.
	+ Protecting confidential and trade secret information.
	+ Detecting and preventing fraud.
	+ Performing identity verification.
	+ Performing accounting, audit, and other internal functions, such as internal investigations.
	+ Complying with the law, legal process, and internal policies.
		- Maintaining records.
		- Claims processing.
		- Responding to legal requests for information and subpoenas; and
		- Exercising and defending legal claims.
* Any other purposes authorized by the California Privacy Protection Agency, State, or Federal law.
* To protect the Bank’s, your or others’ rights, privacy, safety or property (including by making and defending legal claims).
* To prevent, identify, investigate and deter fraudulent, harmful, unauthorized, unethical or illegal activity, including cyberattacks and identity theft.
* To conduct audits relating to interactions, transactions, and other compliance activities.
* To facilitate the creation of, and secure and maintain your account, identify you as a legitimate user in the Bank’s system, provide improved administration, and send you administrative e-mail notifications, such as security or support and maintenance advisories.
* To debug, identify, and repair errors that impair existing intended functionality.
* For short-term, transient use, including, but not limited to, nonpersonalized advertising shown as part of a current interaction with the Bank, provided that the personal information is not disclosed to another third party and is not used to build a profile about you or otherwise alter the experience outside the current interaction with the Bank.
* To perform services on behalf of the Bank, including maintaining or servicing accounts, processing or fulfilling orders and transactions, verifying personnel information, or providing similar services on behalf of the Bank.
* To provide advertising and marketing services, except for cross-context behavioral advertising, to Bank personnel, provided that, for the purpose of advertising and marketing, a service provider or contractor shall not combine the personal information of opted-out personnel that a service provider or contractor receives from, or on behalf of, the Bank with personal information that the service provider or contractor receives from, or on behalf of, another person or persons or collects from its own interaction with personnel.
* To undertake internal research for technological development and demonstration.
* To undertake activities to verify, maintain, or improve the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the Bank.
* For other purposes that are clearly disclosed to you at the time you provide personal information or with your consent.

The Bank has not used or disclosed your sensitive personal information except for those purposes permitted under applicable law.

## Personal Information Disclosures

The Bank may disclose your personal information to the following categories of third parties:

* Bank affiliates to the extent permitted by applicable law.
* Service providers.
* Other third parties, which may include:
	+ Government entities
	+ Operating systems
	+ Banks and other financial institutions
	+ Advertising networks
	+ Internet service providers
	+ Social networks
	+ Data brokers

The Bank may have disclosed any of the above categories of personal information to any of these categories of third parties.

## Personal Information Sales or Sharing

The Bank does not sell or share your personal information. The Bank has no actual knowledge of any sales of personal information for personnel under sixteen (16) years of age.

## Privacy Rights

The CCPA provides California personnel with certain rights:

* To know or access personal information. You may have the right to request access to the personal information the Bank has collected about you.
* To delete personal information. You can request that the Bank delete your personal information, subject to applicable legal obligations.
* To correct personal information. You may have the right to request corrections to any inaccurate or incomplete personal information.
* To limit use or disclosure of sensitive personal information collected. If the Bank uses or discloses sensitive personal information for purposes other than those permitted under applicable law, you can request to limit such activities.
* To opt-out of sharing for cross-contextual advertising. You may opt out of the sale or sharing (as such term is defined under applicable law) of your personal information for cross-contextual behavioral advertising. Such opt-out right may be available through an opt-out preference signal.
* No discrimination or retaliation. You will not be discriminated or retaliated against for exercising your privacy rights.

If you wish to exercise any of these rights, please contact the Bank at customercare@plainscommerce.com or 1-866-937-1134. When making a privacy request, please be prepared to provide: name, address, date of birth, and government issued ID number. The Bank will verify your identity by comparing this information to Bank business records.

Because the Bank does not sell or share the personal information of Bank personnel, the devices, browsers, and other online resources made available to personnel do not respond to opt-out preference signals.

An authorized agent may submit a request on your behalf using the process as described above to exercise your privacy rights. The Bank may request that the agent verify their own identity and/or provide signed permission from you as proof that they are acting as your agent.

## Personal Information Retention

The Bank stores personal information as described in this Policy for a period of seven (7) years, unless a shorter or longer period is appropriate under applicable law, or as necessary to fulfill the purpose(s) for which it was collected, resolve disputes, establish legal defenses, conduct audits, pursue legitimate business purposes, enforce Bank agreements, and comply with applicable laws, or based upon other criteria, including, but not limited to, the relationship between you and the Bank.

## Contact Information

Please contact Plains Commerce Bank, Human Resources Department, HR@plainscommerce.com; 3905 W. 49th Street, Sioux Falls, SD 57106; for inquiries about this Policy.

|  |  |
| --- | --- |
| Author: Chief Risk OfficerPolicy Owner: Chief Risk Officer | Policy Implementation Date: XX/XX/XXXX |
| Revision Date: | Board Approved Date: |
| 9/18/2025 | XX/XX/XXXX |