



## California Consumer Privacy Act Disclosure

Last Updated: June 1, 2023

If you are a California resident, you may have certain rights under the California Consumer Privacy Act (“CCPA”) regarding your personal information. East West Bank and its affiliates (“East West Bank,” “we,” “our,” or “us”) are committed to providing consumers their rights under the CCPA and to protecting the privacy and security of our customers and employees.

Personal information, under the CCPA, is information that identifies, relates to, or could reasonably be linked directly or indirectly with a California resident.

The specific personal information that we collect, use, and disclose covered by the CCPA will vary based on your relationship or interaction with us. The CCPA does not apply to certain information, such as information subject to the Gramm-Leach-Bliley Act (“GLBA”), which is governed by East West Bank’s privacy policy, located on our website or by accessing this link [East West Bank Privacy Policy](#).

This policy provides information about our online and offline practices regarding the collection, use, disclosure, sharing, sale, and retention of personal information. Under the CCPA, the terms “share” and “sale” refer to providing information to a third party for the purposes of advertising and targeted marketing. We do not share or sell information as contemplated by the CCPA. We do disclose information to third parties that we contract with to be able to provide financial services. These third parties may only use information provided for the purposes disclosed in this policy.

### Categories of Personal Information We Collect

We collect personal information to provide financial products and services, and for employment and human resource purposes. The personal information that we collect will depend on our relationship with you. In the preceding 12 months, we have collected the following categories of personal information.

Personal identifiers, such as name, social security/individual tax identification number, government identification number, passport number, driver’s license or state identification number, device identifier, IP address, or user identification (User ID).

Personal information, such as contact information (telephone numbers, addresses, and email address), financial information (including account/loan number, credit and debit card numbers, account balances), medical and health insurance information.

Characteristics of protected classes or groups under state or federal law, such as age, ethnicity and race, marital status, gender, military or veteran status, nationality, citizenship, request for care leave for family or self, including pregnancy leave.

Commercial information, such as products or services purchased, debts, assets, credit history, credit score, account information from other financial institutions, deposit account history, account and loan numbers, balances, debit or credit card number, or transaction histories.

Biometric information, such as fingerprints, health, or medical data.

Internet or other electronic network activity information, such as web cookies.

Geolocation data, such as information used to identify your device location.

Audio and visual, such as audio, electronic, visual (pictures), or similar information, such as call and video recordings.

Employment information, such as work history, salary, years on the job, or current and prior employer.

Education information, such as details about education, school, or degrees earned.

Inferences drawn from any of the information identified above to create a profile about, for example, preferences and characteristics.

Some of the personal information listed above is considered sensitive personal information, such as social security/tax identification number, government identification number, passport number, driver's license or state identification number, account log-in, financial account, debit card or credit card number, credentials to access the account, citizenship or immigration status and racial or ethnic information when required to be collected by law.

## **Sources of Personal Information**

We collect the personal information referenced above from sources which depend on our relationship with you. The information below lists the categories of sources from which we collect personal information.

- Directly from you or an individual acting on your behalf.
- Public records, information made available by federal, state, or local government entities.
- Service providers or other third parties that provide data to support offering financial products and services or employment activities such as fraud prevention, underwriting, completing transactions, supporting our everyday operations, and workforce management. Examples include credit reporting agencies, data aggregating companies, government agencies, other financial institutions, technology providers, and loan brokers.
- Our website or Digital Banking applications.

## **Reasons for Collection and Use of Personal Information**

We collect and use personal information about consumers for the following business or commercial purposes.

To offer and manage products and services, such as

- So that we know who you are and to review qualifications for providing the products and services we offer.
- Supporting the management and maintenance of products and services that we offer, which includes but is not limited to processing transactions, providing statements and account information, and accessing online or mobile banking.

For human resource management, such as

- Identifying and processing employment applicants, including conducting background checks, and verifying qualifications for employment.
- Administering employee services, including pay/compensation.

- Providing benefits to employees and dependents, including healthcare and retirement plans.
- Managing the health and safety of our employees.

To comply with laws and regulations, such as

- Applicable banking, lending, and employment laws, including the Bank Secrecy Act and the Bank Protection Act.
- For us to evaluate our compliance with employment and fair lending laws and regulations.

To provide security, such as

- Using of security cameras to protect you and our employees when on our premises.
- Protecting your account if accessed by a new device and by a device in a new area.

To manage our business and enhance services, such as

- Using cookies to identify your access device to provide you a smoother experience.
- Performing accounting, auditing, and reporting activities and other internal management obligations.
- Complying with our policies, procedures, and contractual or legal obligations.
- Evaluating and engaging in business transactions, which may include mergers, acquisitions, and other transactions such as the transfer or selling of assets.

For marketing, such as

- Communicating with you regarding products and services offered by us, when in compliance with federal and state laws and regulations.
- Use of employee names or images for marketing materials.

## **How We Disclose Personal Information**

We disclose personal information, including sensitive information, about consumers to third parties and service providers. The information below addresses practices in the prior 12 months. The details of the categories of information are detailed in the sections above.

### Personal identifiers

- Vendors and service providers to conduct day-to-day business, including to maintain or service accounts, provide customer service, process payments and transactions, verify customer information, and maintain websites and technology infrastructure.
- Vendors and service providers to conduct activities for human resources related to potential, existing, and former employees.
- Vendors and service providers to assist us in protecting your accounts and personal information, such as account monitoring services for fraud.
- Government agencies and related third parties as required to comply with laws and regulations.

- Third parties to comply with legal and regulatory requirements or provide professional services to us, including auditors, accountants, and legal services.
- Affiliates of East West Bank that may use the personal information consistent with this policy, federal, and state privacy laws.
- Business partners as part of a sale or transfer of business.

#### Personal information

- Vendors and service providers to conduct day-to-day business, including to maintain or service accounts, provide customer service, process payments and transactions, verify customer information, and maintain websites, and technology infrastructure.
- Vendors and service providers to conduct activities for human resources related to potential, existing, and former employees.
- Vendors and service providers to assist us in protecting your accounts and personal information, such as account monitoring services for fraud.
- Government agencies and related third parties as required to comply with laws and regulations.
- Third parties to comply with legal and regulatory requirements or provide professional services to us, including auditors, accountants, and legal services.
- Affiliates of East West Bank that may use the personal information consistent with this policy, federal, and state privacy laws.
- Business partners as part of a sale or transfer of business.

#### Characteristics of protected classes, including sensitive race and ethnicity information

- Vendors and service providers to conduct day-to-day business, including to maintain or service accounts, provide customer service, process payments and transactions, verify customer information, and maintain websites and technology infrastructure.
- Vendors and service providers to conduct activities for human resources related to potential, existing, and former employees.
- Vendors and service providers to assist us in protecting your accounts and personal information, such as account monitoring services for fraud .
- Government agencies and related third parties as required to comply with laws and regulations.
- Third parties to comply with legal and regulatory requirements or provide professional services to us, including auditors, accountants, and legal services.
- Affiliates of East West Bank that may use the personal information consistent with this policy, federal, and state privacy laws.
- Business partners as part of a sale or transfer of business.

#### Commercial information

- Vendors and service providers to conduct day-to-day business, including to maintain or service accounts, provide customer service, process payments and transactions, verify customer information, and maintain websites and technology infrastructure.
- Vendors and service providers to conduct activities for human resources related to potential, existing, and former employees.
- Third parties to comply with legal and regulatory requirements or provide professional services to us, including auditors, accountants, and legal services.

#### Biometric information

- Vendors and service providers to conduct day-to-day business, including to verify customer access to accounts.
- Vendors and service providers to conduct activities for human resources related to potential, existing, and former employees.

#### Internet or other electronic network activity information

- A vendor may be used to help aggregate data that is not related to an individual.
- Vendors and service providers to assist us in protecting your accounts and personal information, such as account monitoring sign-in activity.

#### Geolocation data

- Vendors and service providers to assist with branch locator applications.
- Vendors and service providers to assist us in protecting your accounts and personal information, such as account monitoring sign-in activity.
- Vendors and service providers to assist with activities for human resources.

#### Audio and visual

- Government agencies and related third parties as required if requested by law enforcement.
- Vendors and service providers to assist us in protecting your accounts and personal information.

#### Employment information

- Vendors and service providers to conduct quality control activities.
- Vendors and service providers to conduct activities for human resources related to potential, existing, and former employees.
- Government agencies and related third parties as required to comply with laws and regulations.
- Third parties to comply with legal and regulatory requirements or provide professional services to us, including auditors, accountants, and legal services.
- Affiliates of East West Bank that may use the personal information consistent with this policy, federal, and state privacy laws.
- Business partners as part of a sale or transfer of business.

### Education information

- Vendors and service providers to conduct quality control activities.
- Vendors and service providers to conduct activities for human resources related to potential, existing, and former employees.
- Government agencies and related third parties as required to comply with laws and regulations.
- Third parties to comply with legal and regulatory requirements or provide professional services to us, including auditors, accountants, and legal services.
- Affiliates of East West Bank that may use the personal information consistent with this policy, federal, and state privacy laws.
- Business partners as part of a sale or transfer of business.

### Inferences

- Affiliates of East West Bank that may use the personal information consistent with this policy, federal, and state privacy laws.
- Business partners as part of a sale or transfer of business, generally related to credit worthiness.

## **Share or Sale of Personal Information**

East West Bank does not and will not share or sell the personal information of consumers to third parties as contemplated by the CCPA, including personal information of minors under 16 years of age.

## **Retention of Personal Information**

Personal information is retained as required by regulations and laws, and East West Bank will retain this information as long as is necessary to provide the financial products and services we offer or that are requested by the consumer. All data retained by us is provided with equal protection. It is not used other than how it is described in this policy and as disclosed in our Notice At Collection.

## **Exercising Your Rights**

As a California resident, you have rights related to the personal information we collect, use, and disclose.

- The right to request, free of charge, the following information covering the 12 months preceding your request:
  - The categories of personal information we collected about you.
  - The categories of sources from which the personal information was collected.
  - The purpose for collecting personal information.
  - The categories of third parties to whom we disclosed personal information.
  - The personal information that was disclosed and the purpose for disclosing the personal information, and
  - The specific pieces of personal and sensitive information we collected about you.
- The right to correct inaccurate information.

- The right to delete personal information, subject to certain exceptions.
- The right to non-discrimination in terms of price or service when you exercise a privacy right under CCPA.

Under CCPA, you have the right to opt-out of the sharing or sale of personal information. However, since we do not share or sell information, we do not provide you an opt-out. Technology opt-outs will not be recognized by our website or mobile applications.

## **Making a Request**

East West Bank provides to you three methods to submit a request. The requests will be responded to by our Corporate Office after verification of the requestor's identity and evaluation of the request. Personal information that is protected by other federal privacy laws, such as the Gramm-Leach-Bliley Act ([East West Bank Privacy Policy](#)), Fair Credit Reporting Act, or the Health Insurance Portability and Accountability, is exempt from CCPA requests. We may deny requests related to Personal information that is exempt from CCPA requests. Additionally, we may not delete such exempted personal information when requested. As a financial institution, we are required to maintain personal information to comply with federal and state laws, as well as legal obligations. Although we may not be able to delete information, we will never use personal information in a manner other than you would expect.

If you wish to submit a verifiable request to exercise your rights under the CCPA, you may select from one of these options:

1. Contact us at our toll-free number [888.895.5650](tel:888.895.5650).
2. Complete our [interactive webform](#) or
3. Visit your [local branch](#).

When you request information, we will verify your identity using standard verification methods, utilizing information that we already have about you. This may include personal identifying information about yourself or your accounts with us.

In order to verify your identity, we will review your government issued photo identification, account numbers, card numbers, or other personal identifying information.

Your authorized agent may also make a request on your behalf. When submitting a request on behalf of another person, we may require proof of authorization and verification of identity directly from the person for whom you are submitting a request.

We may change or update this disclosure from time to time. When we do, we will post the revised disclosure on this page with a new "Last Updated" date.

## **Contact for More Information**

For any questions on East West Bank's privacy policies and practices, you may contact us at [info@eastwestbank.com](mailto:info@eastwestbank.com).