

**LOBEL FINANCIAL  
CALIFORNIA EMPLOYEE PRIVACY POLICY**

The State of California requires that we provide privacy information for individuals that are residents of California. If you are not a resident of California, you can disregard this document.

For California residents, here is a summary of what you will learn from this privacy policy:

1. Personal Information We Collect
2. How We Obtain Your Personal Information
3. How Long We Keep Your Personal Information
4. How We Use Your Personal Information
5. How We Disclose Your Personal Information
6. Your Rights Under the CCPA
  - 6.1. Right to Know
  - 6.2. Right to Delete
  - 6.3. Right to Correct
  - 6.4. Right to Limit Use of Sensitive Personal Information
  - 6.5. Right to Opt-Out
  - 6.6. Right to Non-Discrimination
7. Submitting a Request
  - 7.1. How to Submit a Request Yourself
  - 7.2. Authorized Agents
  - 7.3. Response Timing and Delivery Methods
8. Changes to this California Employee Privacy Policy
9. How to Contact Us

**Below is the legal information we are required to share:**

This California Employee Privacy Policy supplements our Employee Handbook and governs the personal information collected, used and shared by Lobel Financial Corporation (“Lobel,” “we,” “us,” or “our”) and applies to job applicants, employees, owners, directors, officers, and contractors of Lobel who are acting in such a capacity (“employment position”) and who reside in the State of California (“consumers” or “you”). We provide these disclosures to comply with the California Consumer Privacy Act of 2018 (“CCPA”). Any terms defined in the CCPA have the same meaning when used in this California Employee Privacy Policy.

**1. PERSONAL INFORMATION WE COLLECT**

We collect information that identifies, relates to, describes, or could reasonably be linked, directly or indirectly, with a particular consumer (“personal information”). Amongst other things, Personal Information does not include publicly available, de-identified, and aggregated information. Information regulated by the Fair Credit Reporting Act is also excluded.

We collect the following categories of personal information:

- “Sensitive Personal Information” such as Social Security Numbers, Driver’s license, financial account or card numbers, precise geolocation, racial and ethnic characteristics, contents of mail, email and text messages, biometric data;
- “Identifiers” such as name, alias, address, unique identifier, internet protocol address, email address, account number, Social Security Number, or government identification number;

- “Other Personal Information” such as name, signature, Social Security Number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, salary information, or any other financial information, or medical information. Some personal information included in this category may overlap with other categories;
- “Protected Characteristics” under California or federal law for classifications such as age (40 years or older), race, color, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), sexual orientation, or veteran or military status;
- “Commercial Information” such as records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies;
- “Internet or Network Activity” such as browsing history, search history, information on a consumer's interaction with a website, application, or advertisement;
- “Geolocation Data” such as physical location or movements;
- “Sensory Data” such as audio, electronic, or visual information;
- “Professional or Employment Related Information” such as current or past job history or performance evaluations;
- “Biometric Information” such as genetic, physiological, behavioral, and biological characteristics, or activity patterns used to extract a template or other identifier or identifying information, such as, fingerprints, faceprints, and keystroke, or gait; and
- “Inferences” drawn from other personal information such as profile reflecting a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

**2. HOW WE OBTAIN YOUR PERSONAL INFORMATION**

Directly from you	You enter or provide us with information in person, online, by email, by phone, by document upload, during COVID-19 return to work procedures  For example, when you apply for a job or update your information on file
Directly and indirectly from you based on activity on our website or network	For example, from internet browsing or network usage details collected automatically
From vendors that interact with us in connection with your employment position	For example, credit reporting agencies from which we check your credit in connection with a submitted employment application, vendors that provide background search results, or vendors that assist in protecting you and us from fraud and identity theft

### **3. HOW LONG WE KEEP YOUR PERSONAL INFORMATION**

Based on legal requirements such as a legal hold, statutory retention periods, or regulatory requirements, human resources personal information is maintained for specified periods of time. The retention clock generally starts when our relationship ends. Our business records where your personal information is imbedded, are excluded from the above. For example, work emails and executed vendor contracts are saved for our business operations for an indefinite period of time.

### **4. HOW WE USE YOUR PERSONAL INFORMATION**

We may use or disclose the personal information we collect for one or more of the following purposes:

1. Performing services on our behalf, including but not limited to:
  - a. To fulfill or meet the reason for which the information is provided.
  - b. To complete background checks.
  - c. To provide you with a decision on an employment application.
  - d. To provide you with employment benefits and process payroll.
  - e. To carry out our obligations and enforce our rights arising from any contracts entered into between you and us.
  - f. To maintain insurance policies and coverages, including for workers' compensation and other liability insurance.
  - g. To manage workers' compensation claims.
  - h. To manage performance of job duties of employees, including compliance with Lobel policies and procedures.
  - i. To communicate with personnel regarding employment-related matters such as upcoming benefits enrollment deadlines, action items, availability of W-2 forms, and other alerts and notifications.
  - j. To assist personnel with the coordination of travel.
2. Helping to ensure security and integrity to the extent the use of the consumer's personal information is reasonably necessary and proportionate for these purposes.
3. Debugging to identify and repair errors that impair existing intended functionality.
4. To implement, monitor, and manage electronic security measures on devices of Lobel personnel that are used to access Lobel networks and systems.
5. Auditing related to a current interaction with you.
6. Undertaking activities to verify or maintain the quality of a service or device controlled by us, and to improve, upgrade, or enhance our services.
7. For short-term, transient uses.
8. To reduce the risk of spreading COVID-19 or other diseases in the workplace, including contact tracing as needed or required by law.
9. To comply with state and federal laws and regulations requiring employers to maintain certain records (such as immigration compliance records, personnel files, wage and hour records, payroll records, accident or safety records, and tax records).
10. To conduct workplace investigations (such as investigations of workplace accidents or injuries, harassment claims, or other alleged misconduct).
11. To provide benefits, services, and perquisites to you.

### **5. HOW WE DISCLOSE YOUR PERSONAL INFORMATION**

We may disclose your personal information to a service provider, contractor, or third party. When we disclose personal information to a service provider or contractor, we enter into a contract that describes the purpose and requires the receiving entity to keep personal information confidential and not use it for any purpose

except performing the services described in the contract or as allowed under the CCPA. Examples of third parties we disclose information to:

- With background search and employment eligibility companies we disclose Sensitive Personal Information, Identifiers, Other Personal Information, Protected Characteristics, Commercial Information, Professional and Employment Information, Inferences;
- With word processing applications, signing vendors, and communication platforms we disclose Sensitive Personal Information, Identifiers, Other Personal Information, Protected Characteristics, Professional and Employment Information;
- With advisors such as attorneys, banks, credit card companies, accountants, financial advisors, consultants, and insurance providers, we disclose Sensitive Personal Information, Identifiers, Other Personal Information, Protected Characteristics, Commercial Information, Internet or Network Activity, Geolocation Data, Sensory Data, Professional or Employment Related Information, Biometric Information, and Inferences;
- With insurance and benefits providers we disclose Sensitive Personal Information, Identifiers, Other Personal Information, Protected Characteristics;
- With education providers we disclose Identifiers, Other Personal Information, Professional or Employment Related Information, and Inferences;
- With building access and security services we disclose Sensitive Personal Information, Identifiers, Other Personal Information, Protected Characteristics, Internet or Network Activity, Geolocation Data, Sensory Data, Professional or Employment Related Information, and Biometric Information;
- With job posting platforms and employment recruiters we disclose Sensitive Personal Information, Identifiers, Other Personal Information, Protected Characteristics, and Professional or Employment Related Information;
- With network monitoring, analytics, and incident response vendors we disclose Sensitive Personal Information, Identifiers, Other Personal Information, Protected Characteristics, Commercial Information, Internet or Network Activity, Geolocation Data, Sensory Data, Professional or Employment Related Information, Biometric Information, and Inferences; and
- With regulatory and governmental agencies we disclose Sensitive Personal Information, Identifiers, Other Personal Information, Protected Characteristics, Commercial Information, Internet or Network Activity, Geolocation Data, Sensory Data, Professional or Employment Related Information, Biometric Information, and Inferences, and when such sharing involves health information, we maintain an employee's anonymity whenever possible.

## **6. YOUR RIGHTS UNDER THE CCPA**

The CCPA provides California residents with specific rights regarding their personal information: the Right to Know, the Right to Delete, the Right to Correct, the Right to Limit use of Sensitive Personal Information, the Right to Opt-Out of the Sale of Personal Information or the Sharing of Personal Information, and the Right to Non-Discrimination. This section describes your CCPA rights and explains how to exercise those rights, if applicable.

### **6.1. Right to Know**

You have the right to request that we disclose certain information to you about our collection, use, and disclosure of your personal information ("Right to Know"). Once we receive and verify your request, unless an exemption applies, we will disclose to you:

- Categories of Personal Information Collected, Disclosed, Sold, and/or Shared:

- The categories of personal information we collected about you
- The sources for the personal information we collected about you
- Our business or commercial purpose for collecting that personal information
- The categories of third parties with whom we disclose that personal information
- If we disclosed your personal information, the categories of personal information disclosed with each category of third-party recipients;
- If we sold or shared your personal information for cross-contextual behavioral advertising, the categories of personal information sold or shared; or
- Specific Information
  - The specific pieces of personal information we collected about you.

## **6.2. Right to Delete**

You have the right to request that we delete any of your personal information that we collected and retained (“Right to Delete”). Once we receive and verify your request, we will delete, de-identify, or aggregate your personal information, unless an exemption or exception applies.

We may deny your Request to Delete if retaining the personal information is necessary for us to:

- Complete the transaction for which the personal information was collected, provide a good or service requested by the consumer, or as reasonably anticipated within the context of our ongoing relationship, or otherwise perform a contract between the us.
- Help to ensure security and integrity to the extent the use of the consumer's personal information is reasonably necessary and proportionate for those purposes.
- Debug to identify and repair errors that impair existing intended functionality.
- Exercise free speech, ensure the right of another consumer to exercise his or her right of free speech, or exercise another right provided for by law.
- To enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business and compatible with the context in which the consumer provided the information.
- Comply with a legal obligation.

## **6.3. Right to Correct**

You have the right to request that we correct your personal information if it is inaccurate (“Right to Correct”). Once we verify your identity and confirm that your personal information is inaccurate, we will correct your personal information.

## **6.4. Right to Limit the Use of Sensitive Personal Information**

You have the right to direct us to limit the use of your sensitive personal information to uses which are necessary to perform the services or provide the goods reasonably expected. However, we only use Sensitive Personal Information in an employment context and as reasonably expected by a consumer.

## **6.5. Right to Opt Out**

If applicable, you have the right to opt out of the 1) sale of personal information, 2) sharing of your personal information, and 3) use of personal information in automated decision-making technology in connection with decisions about the consumer’s work performance, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

We do not sell your personal information. Further, we do not sell the personal information of minors under 16 years of age.

We do not share your personal information. Further, we do not share the personal information of minors under 16 years of age. (“Sharing” means the disclosure of personal information for cross-contextual behavioral advertising.)

We do not process your personal information with automated decision-making.

#### **6.6. Right to Non-Discrimination**

You have the right to not be discriminated against for exercising your rights under the CCPA. Unless permitted by the CCPA, we will not:

- deny you goods or services (including employment opportunities);
- charge you higher prices or rates for goods or services, including through granting discounts or other benefits, or imposing penalties;
- provide you a lower level or quality of goods or services (including employment compensation); or
- suggest that you may receive a different price or rate for goods or services or a different level or quality of goods or services.

### **7. SUBMITTING A REQUEST**

#### **7.1. How to Submit a Request Yourself**

To make a Request to Know, Request to Delete, or Request to Correct, please contact us by either:

- Call us at (833) 906-2155, ask to be transferred to human resources
- Complete this [form](#)

A Request to Know, Request to Delete, or Request to Correct must:

- Provide sufficient information that allows us to reasonably verify you are the person about whom we collected personal information or an authorized representative.
- Describe your request with sufficient detail that allows us to properly understand, evaluate, and respond to it.
- If you are submitting a Request to Know specific pieces of personal information (rather than categories), you will also need to submit a declaration under the penalty of perjury confirming that you are only requesting information about yourself.

Only (1) you or (2) a person authorized by you to act on your behalf, may make a Request related to your personal information.

#### **7.2. Authorized Agents**

Before we can respond to a Request to Know, Request to Delete, or Request to Correct submitted by an authorized agent, we need to verify not only that person or entity’s authority to act on your behalf but also verify the identity of the authorized agent.

If you are authorized to submit a request on behalf of a California resident, please email us at [privacyHR@lobelfinancial.com](mailto:privacyHR@lobelfinancial.com) and provide the following information:

1. To verify your authorization to request on behalf of a California resident, please attach a copy of one or more of the following to your request email:

- signed permission from the California resident (if the agent is an individual), or
  - a valid power of attorney
2. To verify your identity, please attach copies of the following to your request email:
    - valid Government Issued ID (not expired) **AND**
    - a Utility Bill, Bank Statement, or similar documentation to verify your name and address.
  3. To verify the identity of the consumer for whom you are submitting the request, please submit the required information by calling us at (833) 906-2155 (ask to be transferred to human resources); or by emailing us at [privacyHR@lobelfinancial.com](mailto:privacyHR@lobelfinancial.com).

### **7.3. Response Timing and Delivery Method**

We will acknowledge receipt of a Request to Know, Request to Delete, or Request to Correct within 10 business days of its receipt. We will respond to a request within 45 days of its receipt. If we require more time (up to 45 additional days for a total of 90 days from receipt of the request), we will inform you of the reason and extension period in writing. We will deliver our written response by mail or electronically. The response we provide will also explain the reasons we cannot comply with a request, if applicable.

We do not charge a fee to process or respond to your request unless it is excessive, repetitive, or manifestly unfounded. If we determine that the request warrants a fee, we will tell you why we made that decision and provide you with a cost estimate before completing your request.

### **8. CHANGES TO THIS CALIFORNIA EMPLOYEE PRIVACY POLICY**

We reserve the right to amend this California Employee Privacy Policy at our discretion and at any time. If we make changes to this California Employee Privacy Policy, we will notify you by email or through a notice on our HR SharePoint.

### **9. HOW TO CONTACT US**

If you have any questions or comments about this California Employee Privacy Policy, the ways in which we collect and use your personal information, or your rights regarding such use, please do not hesitate to contact us at:

Privacy Support E-Mail:	<a href="mailto:privacyHR@lobelfinancial.com">privacyHR@lobelfinancial.com</a>
Postal Address:	Lobel Financial Attn: Privacy Notice 1150 N. Magnolia Ave. Anaheim, CA 92801

Effective Date 04/24/2023