Your Privacy Rights

Rev. January 26, 2026

Introduction

Welcome to Lead Bank!

We work hard to protect your personal information and ensure your information is kept private and secure. The following privacy policy outlines the types of personal information that Lead Bank ("Lead Bank") collects through our websites and services. It also explains why we collect your information and how we use it.

Privacy is important to Lead Bank. We will never rent or sell your information to anyone. If you have any questions or if you believe that Lead Bank has not adhered to this privacy policy, please send us a note at clientsupport@lead.bank. We reserve the right to amend this privacy policy at our discretion and at any time.

Table of Contents

U.S. Consumer Privacy Notice

FACTS	WHAT DOES LEAD BANK DO WITH YOUR PERSONAL INFORMATION?

Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.
What?	The types of personal information we collect and share depend on the product or service you have with us. This information can include: • Social Security number and account transactions • Checking account information and credit history • Payment history and account balances When you are no longer our customer, we continue to retain and share your information as described in this notice.
How?	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons Lead Bank chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does Lead Bank share?	Can you limit this sharing?
For our everyday business purposes – such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus	Yes	No
For our marketing purposes – to offer our products and services to you	Yes	No
For joint marketing with other financial companies	Yes	No
For our affiliates' everyday business purposes – information about your transactions and experiences	No	We don't share
For our affiliates' everyday business purposes – information about your creditworthiness	No	We don't share
For our affiliates to market to you	No	We don't share
For nonaffiliates to market to you	No	We don't share

Questions?	
	• Call 866-845-9545—our menu will prompt you through your choices • Go to www.lead.bank • Email clientsupport@lead.bank

Who we are

Who is providing this notice?	Lead Bank.

What we do

How does Lead Bank protect my personal information?	To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings. We authorize our employees to get your information only when they need it to do their work, and we require companies that work for us to protect your information.
How does Lead Bank collect my personal information?	We collect your personal information, for example, when you • Apply for a loan or open an account • Show your government-issued ID or use your credit or debit card • Provide employment information We also collect your personal information from others, such as credit bureaus, affiliates, or other companies.
Why can't I limit all sharing?	Federal law gives you the right to limit only • Sharing for affiliates' everyday business purposes – information about your creditworthiness • Affiliates from using your information to market to you • Sharing for nonaffiliates to market to you You should be aware that Lead Bank does not collect or share information for these purposes. State laws and individual companies may give you additional rights to limit sharing. See below for more information on your rights under state law.

Definitions

Affiliates	Companies related by common ownership or control. They can be financial and nonfinancial companies.

	• Our affiliates include others, such as Luna Parent, Inc.
Nonaffiliates	Companies not related by common ownership or control. They can be financial and nonfinancial companies. • Lead Bank does not share with nonaffiliates so they can market to you.
Joint marketing	A formal agreement between nonaffiliated financial companies that together market financial products or services to you. • Our joint marketing partners include third-party financial service platforms for credit cards, loans, and other banking services.

Other important information

Lead Bank is chartered under the laws of the State of Missouri and is subject to regulatory oversight by the FDIC. Any consumer wishing to file a complaint against Lead Bank should contact the FDIC through one of the following means: In person or by U.S. Mail at 1100 Walnut Street; Suite 2100; Kansas City, MO 64106, by telephone at (800) 209-7459, or online at: https://ask.fdic.gov/FDICCustomerAssistanceForm

Several U.S. states, including California, have enacted or will soon enact consumer privacy laws that grant their residents certain rights and require additional disclosures. If you are a resident of California or one of these states, you may have rights granted under the applicable state law.

VT: Accounts with a Vermont mailing address are automatically treated as if they have limited the sharing as described above. For joint marketing, we will only disclose your name, contact information and information about your transactions.

NV: We are providing you this notice pursuant to Nevada law. For more information, contact us at 866-845-9545, or email clientsupport@lead.bank, with "Nevada Annual Notice" in the subject line. You may also contact the Bureau of Consumer Protection, Office of the Nevada Attorney General, 555 E. Washington St., Suite 3900, Las Vegas, NV 89101; telephone number: 702-486-3132; email BCPINFO@ag.state.nv.us.

CA: Accounts with a California mailing address are automatically treated as if they have limited the sharing with nonaffiliates as described above. If you are a California resident and would like to exercise additional choices over your data, please review the California Consumer Privacy Act of 2018 and California Privacy Rights Act of 2020 in the next section.

U.S. State Mandated Privacy Notice at Collection

Several U.S. states, including California, have enacted or will soon enact consumer privacy laws that grant their residents certain rights and require additional disclosures (collectively, "State Privacy Laws"). If you are a resident of one of these states, this section applies to you and supplements the information contained in Lead Bank's Privacy Policy.

As explained in our Privacy Policy, both federal and state laws require us to tell you how we collect, use, share, and protect your personal information. As a result, our data collection practices are generally governed by federal law, including the Gramm-Leach-Bliley Act ("GLBA"). However, certain information collected may be out of scope of federal laws and instead covered by State Privacy Laws. Under the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act ("CPRA") of 2020 and other California laws (collectively, the "CCPA"), this may also include information about employees and employee applicants as well as enterprise data (such as business-to-business).

This notice is intended to provide information required under State Privacy Laws, including the CCPA. This notice applies to the data collection and processing practices of Lead Bank (collectively, "Lead Bank" or "we").

We do not and will not sell consumer personal information in the traditional and colloquial sense of the word sale. We do not use advertising technology on our website, which under some State Privacy Laws may be considered a "sale" or "share" of your information. In the preceding twelve (12) months, we have not "sold" or "shared" consumers' personal information, as defined under State Privacy Laws. We do not engage in targeted advertising.

We also do not offer financial incentives, preferential service agreements, or any other differences in our prices or services in exchange for your data.

Your Privacy Choices and Rights

Under the State Privacy Laws, you may have the following rights, including the right to (1) request to know more about the categories and specific pieces of personal information we collect, use, and disclose and access your personal information, including receive the information in a portable format, (2) request deletion of your personal information, (3) request correction of inaccurate personal information, (4) request to limit the use and disclosure of sensitive personal information, and (5) not be discriminated against for exercising these rights ("Data Subject Requests").

This section describes consumers' rights under the State Privacy Laws and explains how you can exercise those rights with Lead Bank.

Right to Delete

Under certain State Privacy Laws, you have the right to request that we delete any of your personal information that we collected from you and retained, subject to certain exceptions. Once we receive and verify your Data Subject Requests, we will delete your personal information from our records (and direct our service providers to delete your personal information from their records), unless an exception applies.

Certain personal information that we collect and use to provide you with financial services, and which Lead Bank is obligated by federal law and/or regulations to retain, cannot be deleted upon request.

We also may deny your Data Subject Requests to delete if retaining the information is necessary for us or our service providers to:

- Detect security incidents;
- Protect against malicious, deceptive, fraudulent, or illegal activity;

- Assist law enforcement in prosecuting those responsible for such activities; or
- Comply with a legal obligation.

Right to Correction

Under certain State Privacy Laws, you have the right to request that we correct any inaccuracies about your personal information. If we provide you with financial services, you can do so through our application.

Right to Know/Right to Access and Data Portability Rights

Under certain State Privacy Laws, you have the right to request that we disclose certain information to you about our collection and use of your personal information over the past 12 months. Once we confirm your Data Subject Request, we will disclose to you, upon specific request:

- The categories of personal information we collected about you.
- The categories of sources for the personal information we collected about you.
- Our business or commercial purpose for collecting, disclosing, or sharing that personal information.
- The categories of third parties with whom we disclose that personal information.
- The categories of personal information we disclosed or sold to each category of third party.
- The specific pieces of personal information we collected about you.

Right to Limit Use and Disclosure of Sensitive Personal Information

You have the right to request that we limit the use and disclosure of sensitive personal information to the services we provide to you. Lead Bank's current practice is to use the sensitive personal information it collects only for the purpose of providing you with the financial services we offer.

Exercising Your Privacy Choices and Rights

If you are a resident of a state that provides the above rights under State Privacy Laws, you may exercise the rights above by:

- By email: clientsupport@lead.bank
- By phone: 866-845-9545

Each Data Subject Request must:

- Provide sufficient information that allows us to reasonably verify you are the person about whom we collected personal information or an authorized representative. We will make every effort to verify your identity using your email address, but we may request additional information. If an authorized representative is making the request on your behalf, we require documentation showing that the representative has such authority.
- Describe your Data Subject Request with sufficient detail that allows us to properly evaluate and respond to it.

We cannot respond to your Data Subject Request or provide you with personal information if we are unable to verify your identity, or unable to verify the authority for the person making the request as your agent. We will use personal information provided in a verifiable consumer Data Subject Request to verify your identity or authority to make the Data Subject Request, and not for any other purpose.

You may only make a verifiable Data Subject Request for access or data portability twice within a 12-month period.

Response Timing and Format

We will acknowledge your Data Subject Request within 10 days. We attempt to respond to every Data Subject Request within 45 days. If we require more time, we will inform you of the reason and how much additional time we require (up to 90 days in total). Any disclosures we provide may only cover the 12-month period preceding the Data Subject Request's receipt. If we are unable to satisfy your Data Subject Request, or a part of your Data Subject Request, we will explain why. Where required by applicable State Privacy Laws, if we deny your request, you may also have the right to appeal our decision, and we will tell you how to submit an appeal in our response.

We do not charge a fee to process or respond to Data Subject Requests.

Authorized Agent

Only you, or a person you have designated in writing as your authorized agent, or who is registered with the applicable Secretary of State to act on your behalf, or to whom you have provided power of attorney pursuant to applicable laws ("Authorized Agent"), may make a verifiable Data Subject Request. You may also make a verifiable Data Subject Request on behalf of your minor child.

If you wish to have an Authorized Agent make a request on your behalf, they will need to provide us with sufficient written proof that you have designated them as your Authorized Agent, and we will still require you to provide sufficient information to allow us to reasonably verify that you are the person about whom we collected personal information.

Non-Discrimination

We will not discriminate against you for exercising any of your rights. Unless permitted by the State Privacy Laws, we will not:

- Deny you services.
- Charge you different prices for our services, including through granting discounts or other benefits, or imposing penalties.
- Provide you a different level or quality of service.

California Specific Notices

If you are a California resident, California Civil Code Section 1798.83 permits you to request a list of all third parties to which we, during the immediately preceding calendar year, have disclosed certain personally identifiable information for direct marketing purposes. In the preceding calendar year, we have not disclosed personally identifiable information for direct marketing purposes.

We are only required to respond to a customer request for this list once during any calendar year. To make such a request, please see above under the section "Exercising Your Privacy Choices and Rights." Please be aware that not all information sharing is covered by the California privacy rights requirements and only information sharing that is covered will be included in our response.

During the last twelve (12) months, we have collected personal information in the following categories from consumers and disclosed personal information with the following categories of recipients. Although the list contains examples of information collected, we do not collect every specific piece of personal information for every consumer:

Category of Personal Information	Examples of Personal Information Collected	Categories of Recipients
Identifiers	Name, address, email address, phone number, account identifiers, online identifiers, IP address, Social Security number, or other similar identifiers.	Our affiliates, service providers, third parties to whom you or your agents authorize us to disclose your personal information in connection with products or services we provide to you.
California customer records or similar information in states with applicable privacy laws	Name, signature, Social Security number, address, telephone number, driver's license or state identification card number, employment, employment history, bank account number, and other financial information. This category may overlap with other categories.	Our affiliates, service providers, third parties to whom you or your agents authorize us to disclose your personal information in connection with products or services we provide to you.
Characteristics of protected classifications under state or federal law	Age, marital status, or gender.	Our affiliates, service providers, third parties to whom you or your agents authorize us to disclose your personal information in connection with products or services we provide to you.
Commercial information	Purchasing or consuming histories or tendencies.	Our affiliates, service providers, third parties to whom you or your agents authorize us to disclose your personal information in connection with products or services we provide to you.
Internet or other similar network activity	Information on a consumer's interaction with our website, applications, or advertisements.	Our affiliates, service providers, third parties to whom you or your agents authorize us to disclose your personal information in

		connection with products or services we provide to you.
Professional or employment-related information	Current occupation.	Our affiliates, service providers, third parties to whom you or your agents authorize us to disclose your personal information in connection with products or services we provide to you.
Inferences	Inferences drawn from any of the information listed above to create a profile about you, such as a profile that reflects your preferences, characteristics, behavior, and attitudes.	Our affiliates, service providers, third parties to whom you or your agents authorize us to disclose your personal information in connection with products or services we provide to you.
Sensitive Personal Information	Government-issued identifiers (such as Social Security number and driver's license), financial account numbers in combination with login credentials, and facial images used for identification.	Our affiliates, service providers, third parties to whom you or your agents authorize us to disclose your personal information in connection with products or services we provide to you.

We collect personal information for the business and commercial purposes and uses described in the Privacy Policy section titled "What does Lead Bank do with your personal information?"

In addition to the sources described above, we collect personal information from the following categories of sources:

- Directly from our clients or their agents,
- Indirectly from our clients or their agents, in the course of the services that we provide,
- Directly and indirectly from activity on our website,
- Other third-party sources, including government sources, and
- From third parties that interact with us in connection with the services we perform.

The retention periods for data elements within each category listed above vary depending on the nature of the data element and the purposes for which it is collected and used. Our retention period for the data elements within each category is set based on the following criteria: (1) the length of time that the data is needed for the purposes for which it was created or collected, (2) the length of time the data is needed for other operational or record retention purposes, (3) the length of time the data is needed in connection with our legal, compliance and regulatory requirements, for legal defense purposes and to comply with legal holds, (4) how the data is stored, (5) whether the data is needed for security purposes and fraud prevention, and (6) whether the data is needed to ensure the continuity of our products and services.

Changes to Our U.S. State Mandated Privacy Notice at Collection

We reserve the right to amend this privacy notice at our discretion and at any time. When we make material changes to this privacy notice, we will notify you by email, by notice on this site, or by other acceptable means.

Contact Information

If you have any questions or comments about this notice, our Privacy Policy, the ways in which we collect and use your personal information, your choices and rights regarding such use, or wish to exercise your rights under State Privacy Laws, please do not hesitate to contact us.

- By email: clientsupport@lead.bank
- By phone: 866-845-9545

Additional Information for Lead Bank Mobile Users

This section provides additional information about how information is collected, used, and shared when you use the Lead Bank Mobile application (the "Mobile App"). It supplements, and should be read together with, Lead Bank's main Privacy Policy and any other privacy notices we provide to you as a Lead Bank customer.

The Mobile App is currently provided using mobile-banking technology and services from Fiserv, Inc. (sometimes referred to in this section as our "mobile-banking service provider"). Fiserv also publishes a separate TouchBanking Privacy Notice that describes in more detail how its TouchBanking mobile platform collects and uses information. That notice is available at:
https://www.fiserv.com/en/legal/touchbanking-privacy-notice.html

Information Collected When You Use Lead Bank Mobile

In addition to the information described elsewhere in this Privacy Policy (for example, information you provide to open and maintain accounts and to use Lead Bank products and services), the Mobile App, working with our mobile-banking service provider, may collect information from or about you and your device, including:

- Personal information you or Lead Bank provide through the Mobile App, such as your name, address, email address, user IDs, telephone number, and, where necessary, Social Security number, when you enroll in mobile banking or use mobile features.
- Financial and transaction information needed to provide mobile banking services, such as account numbers, payment card details (including expiration date and identification/verification numbers), and transaction and payment history.
- Device images and videos, when you choose to use features that require access to your camera or photo library, such as:
    - Remote check deposit (capturing images of checks); and
    - Using QR codes or similar functionality to initiate peer-to-peer or other payments where available.
- Device contacts, when you choose to use features that allow you to select recipients from your device's contacts (for example, to facilitate peer-to-peer payments where such functionality is

enabled).

- Device and online activity data, such as information about your mobile device (for example, device type, operating system, browser type, IP address, mobile carrier, language and display settings) and your interactions with the Mobile App (for example, pages or screens viewed, access times and duration, navigation within the app). This information may be collected using technologies such as cookies and similar tools, as described in our main Privacy Policy and in Fiserv's TouchBanking Privacy Notice.

- With your permission, the Mobile App and our mobile-banking service provider may collect, access, and use information about the location of your device ("Location Information"). Location Information may be derived from technologies such as GPS, Wi-Fi, cell-tower data and/or IP address, depending on your device settings. We and our mobile-banking service provider may use Location Information for purposes that include:

    - Fraud detection and prevention. For example, Location Information may be used to help detect and prevent card transaction fraud and deposit fraud by comparing the location of your device to the location of an ATM, merchant, or other transaction activity.

    - Providing location-based services. For example, Location Information may be used to:

        - Identify and display nearby Lead Bank branch and ATM locations and related mapping features; and

        - Support other location-based features that may be made available within the Mobile App from time to time.

  You are not required to enable location services to use the Mobile App. If you do not want Location Information to be collected, you can:

    - Decline location access when first prompted by the Mobile App; or

    - Turn off location services for the Mobile App (or for your device entirely) in your device's operating-system settings.

  Please note, however, that if you do not allow the Mobile App to access Location Information, some features may not function properly or may be unavailable, including certain fraud-prevention tools and location-based services (such as branch and ATM locator functions).

Relationship With Fiserv/TouchBanking

Fiserv provides mobile-banking services (including the TouchBanking platform) to Lead Bank as a service provider. When you use Lead Bank Mobile:

- Lead Bank remains responsible for the treatment of your personal information as described in this Privacy Policy and in any other privacy notices we provide to you; and

- Fiserv processes personal information on our behalf to deliver mobile-banking functionality, to support, secure and improve the Mobile App, and for other purposes described in the TouchBanking Privacy Notice and permitted by law and by our agreements with Fiserv.

For a more detailed description of how the TouchBanking platform collects, uses, and shares information (including device-level data and Location Information), you may review Fiserv's TouchBanking Privacy Notice, referenced above. If any aspect of that notice appears to conflict with this Privacy Policy, this "Additional Information for Lead Bank Mobile Users" section and Lead Bank's main Privacy Policy will govern our relationship with you as a Lead Bank customer.