Pinnacle Privacy Practices

Federal law gives consumers the right to limit some of how your personal information is shared. When you interact with us, we may collect and use your personal or sensitive information to better serve you. Read our privacy disclosures to learn more about how we collect, use, and protect your personal or sensitive information.

Have a question about these disclosures? Please visit your local office or contact us at 1-800-264-3613.

FACTS

WHAT DOES PINNACLE 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 income
- Account balances and payment history
- Transaction history and credit history

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 Pinnacle Bank chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does Pinnacle 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	Yes
For joint marketing with other financial companies	No	We don't share.
For our affiliates' everyday business purposes— information about your transactions and experiences	Yes	No
For our affiliates' everyday business purposes— information about your creditworthiness	Yes	Yes
For our affiliates to market to you	Yes	Yes
For nonaffiliates to market to you	No	We don't share.

To limit our sharing

- Call 1-800-264-3613 to notify us of your choice.

Please note:

If you are a *new* customer, we can begin sharing your information 30 days from the date we sent this notice. When you are *no longer* our customer, we continue to share your information as described in this notice.

However, you can contact us at any time to limit our sharing.

Questions?

Call 1-800-264-3613.

Pinnacle℠

What we do	
How does Pinnacle 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.
How does Pinnacle Bank collect my personal information?	We collect your personal information, for example, when you ■ Open an account or apply for a loan ■ Deposit money or pay your bills ■ Tell us about your investment or retirement portfolio 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 credit worthiness ■ affiliates from using your information to market to you ■ sharing for nonaffiliates to market to you State laws and individual companies may give you additional rights to limit sharing.
What happens when I limit sharing for an account I hold jointly with someone else?	Your choices will apply to everyone on your account.

Definitions	
Affiliates	Companies related by common ownership or control. They can be financial and nonfinancial companies. ■ *Our affiliates include companies with a Pinnacle Bank name and includes Pinnacle Financial Partners, Inc.; financial companies such as Pinnacle Advisory Services, Inc. and Miller Loughry Beach, Inc.; and nonfinancial companies such as PFP Title Company, PNFP Holdings, Inc., PNFP Properties, Inc., Pinnacle Service Company, Inc., Pinnacle Rutherford Towers, Inc., Pinnacle Rutherford Real Estate, Inc., Pinnacle Nashville Real Estate, Inc., and Pinnacle Community Development, Inc.*
Nonaffiliates	Companies not related by common ownership or control. They can be financial and nonfinancial companies. ■ *Pinnacle 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. ■ *Pinnacle Bank doesn't jointly market.*

What does this policy cover?

Pinnacle's Digital Privacy Practices ("Privacy Policy") describes how we collect and share information when you visit and/or use Pinnacle's website, mobile applications and other online services ("Digital Services").

Our Digital Services are intended for a U.S. audience and may be accessed globally as a service to our U.S. clients. The terms "Pinnacle," "we," "us" or "our" mean Pinnacle Bank and its U.S. affiliates. "You" means an individual who visits our Digital Services and does not refer to a business or other entity or individual outside of the U.S.

If you do not agree with our policy and practices, please do not use our Digital Services, or provide us your personal or sensitive information.

What isn't covered by this policy?

This Privacy Policy does not apply to the websites, mobile applications or services of Pinnacle's businesses and affiliates that do not directly link to this policy. Some Pinnacle businesses and affiliates have their own privacy policies, which can be found on their websites. It also does not apply to non-Pinnacle companies, such as third-party or service provider websites to which we link online. Please review the privacy policies of other websites and services you visit to understand their privacy practices.

How does Pinnacle use collected information?

The information we collect through our Digital Services helps Pinnacle do the following:

- Manage your account (process transactions, respond to product applications and questions);
- Fulfill our regulatory requirements;
- Analyze our site usage and how it is being accessed and used; improving functionality; and enhancing the user's experience;
- Send marketing and other communications;
- Prevent and detect fraud;
- Protect against risks to security (protect against malicious, deceptive or illegal activity); or
- Carry out other day-to-day business operations.

To protect your personal or sensitive information from unauthorized access and use, we use security measures that comply with federal law. These security measures include computer safeguards; secured files and buildings; detecting security incidents; and protecting our Digital Services against fraudulent and illegal activity.

The application information is retained in accordance with state and federal record retention laws. Please contact us to determine specific timeframes for your personal stored information and if that information may be deleted.

What information does Pinnacle collect?

When using our Digital Services, the applications may request access to information stored on your data such as location, camera, contacts, or other features you are enrolled in to enrich and simplify your own user experience and improve our services, as well as provide additional security to protect your account. Before granting access to this information, you are prompted to give that application permission. Should you wish to not grant permission, you may decline permission.

The table below describes categories of personal or sensitive information and some examples of these categories that we may collect from you when you visit/use a Pinnacle website or application or interact with us online:

Category	Examples
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.*
Camera/Images	*Use of your camera to capture a check image for mobile deposit*
Contacts	*A contact to use with features that allow you to send money via your mobile application. We will only add the contacts you choose, and that information will not be shared*
Geolocation data	*Such as a device location, login information, and Internet Protocol (IP) location*
Identifiers	*A real name, alias, postal address, unique personal identifiers, online identifier, Internet Protocol address, cookies, flash cookies, direct identifiers, web beacon, email address, account name, Social Security number, driver's license number, passport number or other similar identifiers.*
Inferences drawn from other personal or sensitive information	*A profile reflecting a person's preferences, such as characteristics.*
Internet or other similar network activity	*Browser type, browsing history, search history and information on a consumer's interaction with a website, application or advertisement.*
Personal or Sensitive information	*A name, Social Security number, address, telephone number, driver's license or state identification card number, employment, bank account number, credit card number, debit card number or any other financial information. Some personal or sensitive information included in this category may overlap with other categories.*
Protected classification characteristics	*Age, race, color, citizenship, religion or creed, marital status, physical or mental disability, veteran or military status, genetic information.*
Sensory data	*Audio, electronic, visual, thermal or similar information.*

Other important notices

Our Consumer Privacy Notice applies to information that we collect about individuals who seek, apply for or obtain our financial products and services for personal, family or household purposes. Our California Consumer Privacy Notice (CCPA Notice) applies to certain information we collect about California residents. You can find these notices here.

Questions/Contact Us

Pinnacle's business address is Pinnacle Financial Partners, 150 Third Avenue South, Suite 900, Nashville, TN 37201, USA. Our Client Service Center can be reached toll-free at 800.264.3613.

This Privacy Notice for California Residents is provided by Pinnacle Bank, a Tennessee Bank, and its subsidiaries and affiliates, including Pinnacle Financial Partners ("we" or "us") pursuant to the California Consumer Privacy Act of 2018 ("CCPA") and supplements the information contained in Pinnacle Bank's Privacy Notice.

This notice applies solely to consumers who reside in the State of California ("consumers" or "you"), and to "personal or sensitive information" as defined in the CCPA. However, as used in this notice, the term "personal or sensitive information" does not include, and this notice does not apply to:

- Personal or sensitive information that we collect, process, sell, or disclose pursuant to the federal Gramm-Leach-Bliley Act, and implementing regulations, or the California Financial Information Privacy Act (Division 1.4 (commencing with Section 4050) of the Financial Code);
- Publicly available information from government records;
- De-identified or aggregated consumer information; or
- Other information excluded from the CCPA's scope, including:
    - Health or medical information covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the California Confidentiality of Medical Information Act (CMIA) or clinical trial data;
    - Personal or sensitive information covered by other sector-specific privacy laws, including the Fair Credit Reporting Act (FRCA) and the Driver's Privacy Protection Act of 1994.

I. Personal or Sensitive Information We Collect

The table below describes the categories of personal or sensitive information, and some examples of those categories that we may have collected from consumers within the last twelve (12) months:

Category	Examples
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.*
Camera/Images	*Use of your camera to capture a check image for mobile deposit*
Contacts	*A contact to use with features that allow you to send money via your mobile application. We will only add the contacts you choose, and that information will not be shared*
Geolocation data	*Such as a device location, login information, and Internet Protocol (IP) location*
Identifiers	*A real name, alias, postal address, unique personal identifiers, online identifier, Internet Protocol address, cookies, flash cookies, direct identifiers, web beacon, email address, account name, Social Security number, driver's license number, passport number or other similar identifiers.*
Inferences drawn from other personal or sensitive information	*A profile reflecting a person's preferences, such as characteristics.*
Internet or other similar network activity	*Browser type, browsing history, search history and information on a consumer's interaction with a website, application or advertisement.*
Personal or Sensitive information	*A name, Social Security number, address, telephone number, driver's license or state identification card number, employment, bank account number, credit card number, debit card number or any other financial information. Some personal or sensitive information included in this category may overlap with other categories.*
Protected classification characteristics	*Age, race, color, citizenship, religion or creed, marital status, physical or mental disability, veteran or military status, genetic information.*
Sensory data	*Audio, electronic, visual, thermal or similar information.*

II. Sources of Personal or Sensitive Information

We might obtain the categories of personal and/or sensitive information listed above from the following categories of sources:

- Directly from you. For example, from forms you complete or products and services for which you apply or that you obtain from us.
- From others, such as credit bureaus, affiliates, or other companies.

III. Use of Personal or Sensitive Information

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

- To fulfill the purposes for which 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 or sensitive information to respond to your inquiry.
- If you provide your personal or sensitive information to apply for employment or in the context of your employment, including for purposes of obtaining or maintaining benefits, we will use that information for those purposes.
- To provide, support, personalize, and develop our Website, products, and services.
- 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.
- To respond to law enforcement requests and as required by applicable law, court order, or governmental regulations.
- As described to you when collecting your personal or sensitive 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 or sensitive information held by us about our Website users is among the assets transferred.

IV. Sharing Personal or Sensitive Information

We may share personal or sensitive information we collect about California residents to operate, manage, and maintain our business and to provide our products and services. When we disclose personal or sensitive information for a business purpose, we may enter into a contract that describes the purpose and requires the recipient to both keep that personal or sensitive information confidential and not use it for any purpose except performing service the contract.

We may share your personal or sensitive information with the following categories of third parties:

- Service providers.
- Affiliates.
- Third parties to whom you or your agents authorize us to disclose your personal or sensitive information in connection with products or services we provide to you.

V. Sales of Personal or Sensitive Information

We do not offer an opt-out from the sale of personal or sensitive information because we do not engage in the sale of personal or sensitive information as contemplated by the CCPA. We have not sold personal or sensitive information subject to the CCPA, which includes personal or sensitive information of minors under the age of 16, nor does Bank intend to sell personal information. The CCPA defines a "sale" as the disclosure of Personal or sensitive information for monetary or other valuable consideration.

VI. Disclosures of Personal or sensitive information for a Business Purpose

During the past 12 months, we may have disclosed the categories of Personal or sensitive information listed above for our business purposes.

VII. Your Rights and Choices

The CCPA provides California consumers with specific rights regarding their personal information. This section describes your CCPA rights and explains how to exercise those rights.

Access to Specific Information and Data Portability Rights

You have the right to request that we disclose certain information to you about our collection, use, and disclosure of your personal or sensitive information over the past 12 months. Once we receive and confirm your verifiable consumer request (see *Exercising Access, Data Portability, and Deletion Rights*), we will disclose to you:

- The categories of personal or sensitive information we collected about you.
- The categories of sources for the personal or sensitive information we collected about you.
- Our business or commercial purpose for collecting that personal information.
- The categories of third parties with whom we share that personal information.
- The specific pieces of personal or sensitive information we collected about you (also called a data portability request).
- The categories of personal or sensitive information about you that we disclosed for a business purpose, to the extent we have made such disclosures.

Deletion Request Rights

Subject to certain exceptions, you have the right to request that we delete the personal or sensitive information that we collected about you. Once we receive and confirm your verifiable consumer request (see *Exercising Access, Data Portability, and Deletion Rights*), we will delete (and direct our service providers to delete) your personal or sensitive information from our records, unless an exception applies.

We may deny your deletion request if retaining the information is necessary for us or our service provider(s) to:

1. Complete the transaction for which we collected the personal information, provide a good or service that you requested, take actions reasonably anticipated within the context of our ongoing business relationship with you, or otherwise perform our contract with you.
2. Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for such activities.
3. Debug products to identify and repair errors that impair existing intended functionality.
4. Exercise free speech, ensure the right of another consumer to exercise their free speech rights, or exercise another right provided for by law.
5. Comply with the California Electronic Communications Privacy Act (Cal. Penal Code § 1546 *et. seq.*).
6. Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the information's deletion may likely render impossible or seriously impair the research's achievement, if you previously provided informed consent.

7. Enable solely internal uses that are reasonably aligned with consumer expectations based on your relationship with us.
8. Comply with a legal obligation.
9. Make other internal and lawful uses of that information that are compatible with the context in which you provided it.

Exercising Access, Data Portability, and Deletion Rights

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

- Calling us at 1-800-264-3613
- Visiting https://www.pnfp.com/contact-us/ and select the “Email Us” tab. In the web-form dropdown menu, choose "Privacy." In your message, you must include your telephone number for us to process your request.

Only you, or a person registered with the California Secretary of State that you authorize 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.

You may only make a verifiable consumer request for access or data portability twice within a 12-month period. The verifiable consumer request must:

- Provide sufficient information that allows us to reasonably verify you are the person about whom we collected personal or sensitive information or an authorized representative.
- Describe your request with sufficient detail that allows us to properly understand, evaluate, and respond to it.

Making a verifiable consumer request does not require you to create an account with us.

We will only use personal or sensitive information provided in a verifiable consumer request to verify the requestor's identity or authority to make the request.

Response Format

We will deliver our written response by mail or electronically, to you at your option.

Any disclosures we provide will only cover the 12-month period preceding the verifiable consumer request's receipt. The response we provide will also explain the reasons we cannot comply with a request, if applicable. For data portability requests, we will select a format to provide your personal or sensitive information that is readily useable and should allow you to transmit the information from one entity to another entity without hindrance.

We do not charge a fee to process or respond to your verifiable consumer 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 we reserve the right to either refuse to act on your request or charge you a reasonable fee to complete your request if it is excessive, repetitive, or manifestly unfounded.

Non-Discrimination

You have a right to not receive discriminatory treatment for exercising your CCPA rights. Except to the extent permitted by CCPA, we will not discriminate against you for exercising any of your CCPA rights, including by:

- Denying you goods or services;
- Charging you different prices or rates for goods or services, including through granting discounts or other benefits, or imposing other similar penalties;
- Providing you a different level or quality of goods or services; or

- Suggesting that you may receive a different price or rate for goods or services or a different level or quality of goods or services.

VIII. Changes to Our Privacy Notice

We reserve the right to amend this privacy notice at our discretion and at any time. When we make changes to this privacy notice, we will post the updated notice on the Website and ensure the notice is updated to reflect the revision date.

Your continued use of our Website following the posting of changes constitutes your acceptance of such changes.