Rev. 10/22/2026

FACTS	WHAT DOES PIBANK DO WITH YOUR PERSONAL INFORMATION?
Why?	This Privacy Notice applies to Pibank, N.A. ("Pibank") and its affiliates. It applies to all the products and services offered to U.S. Consumers. 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? **How?**	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 or loss/default history and credit history ■ Biometric and identity-verification information, including a photograph of you (a "selfie"), an image of your government-issued identification, and the facial measurements (facial geometry) generated from those images to verify your identity
	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 Pibank chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does Pibank 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.	Yes	No
For our affiliates' everyday business purposes - information about your creditworthiness.	Yes	Yes
For our affiliates to market to you.	Yes	Yes
For non-affiliates to market to you.	No	We don't share

To limit our sharing	**Please select your opt-in or opt-out decision during onboarding or provide us an update via your Pibank App.** If you are a new customer, we can begin sharing your information thirty (30) days from the date we issue 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 (954) 636-7777 or Toll Free 1(877) 678-0888 or visit www.pibank.com.

Who we are	
Who is providing this notice?	This notice is provided by Pibank N.A.
What we do	
How does Pibank 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 also maintain other physical, electronic and procedural safeguards to protect this information and we limit access to information to those employees for whom access is appropriate.
How does Pibank collect my personal information?	We collect your personal information, for example, when you ■ open an account or make a deposit or a withdrawal from your account; ■ pay your bills or apply for a loan; ■ use your credit or debit card. ■ Open an account, sign in on a new device, change your password, or authorize a payment, transfer, or other transaction through the Pibank mobile banking app, at which time we and our identity-verification service provider collect a selfie and an image of your government-issued identification and generate facial measurements to verify your identity. We also collect your personal information from others, such as credit bureaus, affiliates or other companies.
What biometric and identity-verification information do we collect?	When you use the Pibank mobile banking app, we and our identity-verification service provider, authID Inc. ("authID"), may collect: - A live photograph of your face (a "selfie") captured through your device camera, and the facial measurements (facial geometry) generated from it; - An image of your government-issued identification (such as a passport, driver's license, or U.S. state identification card), including the photograph on it; information extracted from it, such as your name, address, date of birth, nationality, document type and number, and issue and expiration dates; and, if your document supports it,

	information read from the document's embedded chip; - Liveness-detection information used to confirm that the selfie is of a live person and not a photograph, video, or other spoof; - A facial biometric template that authID derives from your enrolled selfie and stores in a proprietary, encrypted form that cannot be reversed into your original facial image; and - Information about each verification, such as the date and time, transaction identifier, verification result, device and network information, and fraud or liveness indicators, together with your name, mobile phone number, email address, and a unique user identifier (not your account number) that authID maintains to provide its services.
When and why do we collect it?	We use authID facial verification only for identity verification, fraud prevention, account security, authorization of sensitive banking activity, and compliance with our legal and regulatory obligations, including federal customer identification requirements. We collect this information when you: - Open an account, when we verify your government-issued identification and compare your selfie to the photograph on it; - Sign in from a new device, or recover or change your login credentials (including through Login > Get Help); - Authorize a payment order, transfer, or other higher-risk or significant-value transaction; - Update your know-your-customer information, or re-verify your identity when the identification document we have on file has expired; and - Confirm other security-sensitive actions in the app. For actions after account opening, the app captures a new live selfie, and authID compares it to your enrolled facial biometric template.
How is Apple Face ID different?	If you choose to enable Apple Face ID to unlock the app, that authentication is performed locally on your device by Apple. Pibank does not collect, receive, store, or have access to the facial images, facial maps, or biometric templates maintained by Apple, and the app receives only a success or failure result.

How do we obtain your consent?	Before any facial image is captured and transmitted to authID, we show you a clear disclosure and ask for your explicit consent. During biometric enrollment, you are also presented with authID's own Privacy Notice and Terms and Conditions, which provide additional detail about authID's collection, use, sharing, security, retention, and deletion of facial images and associated biometrics.
Who do we share my biometric and identity-verification information with?	We share your selfie, your identification image and information, liveness information, and related biometric information with authID. authID acts as our identity-verification service provider and processes this information on our behalf to perform identity verification, authentication, liveness detection, and fraud prevention. At our direction, authID may send information from your identification document to third-party document-authentication services that check the document and its data against commercial or government databases. Our agreements with authID limit its use and disclosure of this information to providing services to us, require it to safeguard the information, and prohibit it from selling the information or making it available to other third parties, other than the document-authentication service providers described above that act on our behalf. We may also disclose this information when required by law, such as in response to a subpoena or court order. Neither we nor authID sell your face data or disclose it to advertisers, advertising networks, or data brokers, and we do not use your face data for advertising, marketing, cross-app tracking, or unrelated profiling.
Where is my biometric and identity-verification information stored, and how is it protected?	authID processes and stores biometric information using Microsoft Azure cloud infrastructure. Face data is encrypted while it is transmitted and protected by encryption while it is stored. The Pibank app does not store your facial biometric template or facial images on your device. When you open an account, we receive from authID the results of the identity verification, together with the identification information and images captured during onboarding, and we keep them with our account-opening records as required by law. For verifications after account opening, we receive only an approved or rejected result, and we do not have access to the facial biometric template that authID derives.
How long do we keep my biometric and identity-verification information?	authID keeps your enrolled facial biometric template only while your Pibank digital-access profile remains active and secure app access continues to be necessary. Closing a Pibank deposit account does not necessarily end your digital-access profile, because former customers may still need app access to retrieve account statements, tax

	documents, notices, transaction history, and other records associated with a former banking relationship. authID deletes the other onboarding information it collects within seven (7) days after delivering it to us, except as described above. When your digital-access profile is closed, or the information is no longer needed for identity verification, fraud prevention, or our legal and regulatory obligations, we will instruct authID to delete your facial biometric template. Identification information and images that we keep with our account-opening records are retained for the periods required by federal recordkeeping laws and our record-retention policy, and are then securely destroyed.
Can I withdraw my consent or request deletion of my biometric information?	Yes. If you have questions about your biometric or identity-verification information, or if you wish to withdraw your consent or request deletion of your facial biometric template, call (954) 636-7777 or Toll Free 1(877) 678-0888. If you withdraw your consent, you may use the alternative verification method we offer, such as a one-time passcode or a video call with our staff, although some requests may take longer to complete. We will honor your request to the extent consistent with our legal and regulatory retention obligations and the identity-verification services you have asked us to provide. Withdrawing consent does not require us to delete records that federal law requires us to keep.
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 non-affiliates 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—unless you tell us otherwise.
Definitions	
Affiliates	Companies related by common ownership or control. They can be financial and nonfinancial companies. These include Intercredit Bank, N.A., Banco Pichincha Holding Group, Banco Pichincha Ecuador, Banco Pichincha Panama, Diners Club Ecuador, Banco Pichincha Spain, Banco Pichincha Colombia, Banco Pichincha Peru, Banco de Loja, Diners Club Peru, BP Miami Agency and Banco General Ruminahui.

Nonaffiliates	Companies not related by common ownership or control. They can be financial and non-financial companies. ■ Pibank N.A. does not share with non-affiliates so they can market to you.
Joint Marketing	A formal agreement between nonaffiliated financial companies that together market financial products or services to you. ■ Joint marketing partners include financial services companies.

Other important information

This Privacy Notice applies only to financial products or services that you may obtain with the Pibank or Pibank USA brand. Any consumer personal information collected, processed, or disclosed is pursuant to the federal Gramm- Leach-Bliley Act (Public Law 106-102), and implementing regulations. You may have privacy protections under applicable law and to the extent applicable; we will comply with those provisions.

For Vermont Customers: Accounts with a Vermont mailing address are automatically treated as if they have limited the sharing as described on page 1. For joint marketing, we will only disclose your name, contact information and information about your transactions.

For Nevada Customers: We are providing you this notice pursuant to state law. We will automatically place you on our internal Do Not Call List and you will not receive any marketing calls from us. You may also contact the Nevada Attorney General's office: Bureau of Consumer Protection, Office of the Nevada Attorney General, 555 E. Washington St., Suite 3900, Las Vegas, NV 89101; telephone number: 1-702-486- 3132; email BCPINFO@ag.state.nv.us.

For California Customers: In accordance with California law, we will not share information we collect about California residents with nonaffiliates, unless the law allows. For example, we may share information with your consent or to service your accounts. We will limit sharing among our companies to the extent required by California law.