thrivent®
Bank

Online Privacy Policy

Effective: June 1st, 2025

At Thrivent Bank ("Bank," "we," "us," or "our"), we are committed to protecting your privacy and the security of your personal information. This Online Privacy Policy ("Policy") explains how we collect, use, share, and protect information when you visit our website(s) or use our mobile application(s) (collectively, our "Online Services").

This Policy describes your choices regarding your information and how you can exercise your privacy rights. Please read this Policy carefully to understand our practices. By accessing or using our Online Services, you acknowledge that you have read, understood, and agree to be bound by the terms of this Policy. If you do not agree with our practices, please do not access or use our Online Services.

Definitions

- Affiliate: “Affiliate” means any company that controls, is controlled by, or is under common control with Thrivent Bank
- Aggregate Data/Aggregated Information: "Aggregate Data” or “Aggregated Information” means information that relates to a group or category of individuals, from which individual identities have been removed, and that is not linked or reasonably linkable to any individual or household, including via a device. Aggregate data does not constitute Personal Information.
- Bank/We/Us/Our: "The terms “Bank” “we,” “us,” or “our” refer to Thrivent Bank.
- Biometric Information: "'Biometric Information” means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual.
- CCPA/CPRA: “CCPA” means the California Consumer Privacy Act of 2018, as amended. “CPRA” means the California Privacy Rights Act of 2020, which amends and expands the CCPA.
- Cookies: "'Cookies” are small text files that are placed on your computer or device by websites that you visit. They are widely used to make websites work, or work more efficiently, as well as to provide information to the owners of the site.
- Customer: “Customer” means any individual that has a relationship with the Bank.

- Data Subject: “Data Subject” means an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- Nonpublic Personal Information (NPI): “Nonpublic Personal Information” or “NPI” means personally identifiable financial information. NPI does not include publicly available information.
- Online Services: “Online Services” means Thrivent Bank's website(s) and mobile application(s).
- Personal Information: “Personal Information” means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or household.
- Sale/Sell: “Sale” or “Sell” means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for monetary or other valuable consideration.
- Service Provider: “Service Provider” means a person or entity that processes personal information on behalf of Thrivent Bank and to which Thrivent Bank discloses a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the person or entity receiving the personal information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract, or as otherwise permitted by law.
- Share/Sharing: “Share” or “Sharing” means sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for cross-context behavioral advertising, whether for monetary or other valuable consideration.
- Third Party: “Third Party” shall mean any legal entity, other than Thrivent or a service provider.

Information We Collect

Thrivent Bank collects information about you from several sources when you interact with our Online Services (website and mobile applications), apply for or use our products and services, and as necessary to operate our business. We are committed to

collecting only the minimum necessary information required for legitimate business purposes.

Information You Provide Directly to Thrivent Bank

This section includes information you provide directly to Thrivent Bank's own systems or personnel, not through a third-party platform's interface, even if accessed via a Thrivent Bank link.

Account Credentials

You will create a username and password. Your password is encrypted and stored securely. Thrivent Bank employees do not have access to your plain-text password.

Contacting Customer Support (Directly)

- Information You Provide: Any information you provide to our customer service representatives directly (via phone, email directly to a Thrivent Bank address, a chat function hosted on Thrivent Bank's own systems, or other channels directly controlled by Thrivent Bank), including the nature of your inquiry and any supporting documentation.
    - Call Recordings: We may record phone calls for quality assurance, training, and record-keeping purposes. You will be notified at the beginning of the call if it is recorded.
    - Chat Transcripts: If the chat is hosted directly by Thrivent Bank, we retain transcripts of online chat conversations for quality assurance, training, and record-keeping purposes.
    - Surveys and Promotions (Directly Hosted): Any information you choose to provide in response to surveys, contests, or promotional offers hosted directly by Thrivent Bank.
- User Generated Content
- Feedback Forms

Information You Provide Through Our Online Services, Processed by Our Service Providers

- Account Applications and Loan Applications: When you apply for an account or loan through our Online Services, you may be providing information directly to our service providers' platforms.
- Our core banking platform collects and processes information necessary to open and maintain your accounts, process transactions, and provide banking services. This may include:

    - Identifiers: Your full name, alias, postal address, email address, phone number, date of birth, Social Security number (SSN) or other government-issued identification number.
    - Financial Information: Your income, assets, liabilities, employment information, and other information needed to assess your eligibility for products and services and comply with legal requirements.
    - Beneficiary Information: Names, contact information, and other details about your designated beneficiaries.
    - Transaction Data: Details of all deposits, withdrawals, transfers, and payments.
- If you apply for a loan (mortgage, HELOC, etc.) through our Online Services, you may be providing information directly to our loan origination platform provider. This information may include:
    - Personal Identifiers: As listed above.
    - Financial Information: Detailed financial information, including income, assets, liabilities, credit history, employment history, and information related to the loan purpose.
    - Property Information: Information about the property being financed.

Information Collected Automatically Through Our Online Services

Website Usage Data

- We collect information about your activity on our website, including:
    - Pages visited and features used.
    - Date and time of access.
    - Referring/exit pages (the websites you visited before and after ours).
    - Search terms used (within our site, if applicable).
    - Links clicked.
    - Other interactions with our website content.

Mobile App Usage Data

- We collect information about your activity within our mobile application, including:
    - Features used.
    - Screens viewed.
    - Time spent in the app.
    - Crash reports and diagnostic data (to help us identify and fix technical issues).
    - In-app interactions.

Device Information

- We collect information about the device you use to access our Online Services, including:
    - Device type (e.g., iPhone, Android phone, desktop computer).
    - Operating system and version (e.g., iOS 16, Android 13, Windows 11).
    - Unique device identifiers (e.g., Device ID, Advertising ID). Note: You can typically limit the use of advertising IDs through your device settings. See the "Your Data Subject Rights" section for more information.
    - Mobile network information (e.g., carrier, network type).
    - IP address (which may provide general location information).

Mobile App Permissions

- Phone Number: The app may request access to your phone number to facilitate secure login, account verification, or to enable certain features. We will always request your permission before accessing your phone number.
- Contacts: The app may request access to your contacts to facilitate features such as person-to-person payments (e.g., sending money to someone in your contact list). We will only access your contacts with your explicit permission, and we will only use this information for the specific purpose(s) for which you granted access. We do not store your entire contact list on our servers.

Information We Receive from Other Third Parties

In addition to the information, you provide directly to us and the information we collect automatically, Thrivent Bank may also receive information about you from other third-party sources, as permitted by law. We use this information to supplement the information we already have, to improve our services, to comply with legal obligations, and for other purposes described in the "How We Use Your Information" section.

- Credit Bureaus: When you apply for a loan or credit product, we may obtain your credit report and credit score from one or more consumer reporting agencies (such as Experian, Equifax, and TransUnion). This information is used to assess your creditworthiness and make lending decisions. We obtain this information with your authorization, as required by the Fair Credit Reporting Act (“FCRA”).
- Fraud Prevention Services: We may use third-party fraud prevention services to verify your identity, prevent fraudulent transactions, and protect against account takeover. These services may provide us with information such as:
    - Device risk scores.
    - IP address reputation.
    - Information about known fraudulent activity associated with your email address or phone number.
    - Verification of identity information.

- Marketing Partners
    - We may receive information about you from marketing partners with whom we offer co-branded services or engage in joint marketing activities. This information may include your name, contact information, and information about your interests. We will only receive this information if you have provided your consent to the marketing partner or if otherwise permitted by law.
- Affiliates
    - We may collect information from Thrivent, the parent company.

Biometric Information

If you choose to use biometric login features (fingerprint or facial recognition) within our mobile application, the authentication process is handled by your device's operating system. Thrivent Bank does not collect, store, or have access to your biometric data itself.

Geolocation Information

Geolocation data is not collected or transmitted while using the Thrivent Bank mobile app, located on the Google Play Store and on Apple’s App Store.

Geolocation data such as device location and your IP address is collected when visiting our website.

Personal Information Collected and Data Retention

To provide you with a clearer understanding of our data practices, the table below summarizes the categories of personal information we may collect, provides examples of each category, indicates whether Thrivent Bank collects that category of information, and describes our general retention practices.

Thrivent Bank retains your personal information only for as long as necessary to fulfill the purposes for which it was collected, as described in this Policy, and to comply with applicable laws, regulations, and our internal recordkeeping requirements.

- We retain information for as long as necessary to provide you with our services, manage your accounts, resolve disputes, enforce our agreements, and for other legitimate business purposes.
- We retain information as required by contracts with our service providers and other third parties.
- In the event of litigation, legal claims, or government investigations, we may need to retain information for longer than the standard retention periods. A legal hold supersedes the retention schedule.

Category[1]	Examples	Collected	Retention Period
A. Identifiers	A real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, Social Security number, driver's license number, passport number, or other similar identifiers.	Yes	For the duration of your relationship with us plus any legal or regulatory retention period.
B. Personal Information	A 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, or any other financial information, medical information, or health insurance information. Some personal information included in this category may overlap with other categories.	Yes	For the duration of your relationship with us plus any legal or regulatory retention period.

[1] Categories of personal information are as defined in Cal. Civ. Code. § 1798.140(v) (effective Jan. 1, 2023).

Category[1]	Examples	Collected	Retention Period
C. Protected Classification Characteristics Under California or Federal Law	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, veteran or military status, genetic information (including familial genetic information).	Yes	For the duration of your relationship with us plus any legal or regulatory retention period.
D. Commercial Information	Records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.	No	N/A
E. 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, faceprints, and voiceprints, iris or retina scans, keystroke, gait, or other physical patterns, and sleep, health, or exercise data.	No	N/A
F. Internet or Other Similar Network Activity	Browsing history, search history, information on a consumer's interaction with a website, application, or advertisement.	Yes	For the duration of your relationship with us plus any legal or regulatory retention period.
G. Geolocation Data	Physical location or movements.	Yes (excluding Mobile App)	For the duration of your relationship with us plus any legal or regulatory retention period.

Category[1]	Examples	Collected	Retention Period
H. Sensory Data	Audio, electronic, visual, thermal, olfactory, or similar information.	Yes	For the duration of your relationship with us plus any legal or regulatory retention period.
I. Professional or Employment-Related Information	Current or past job history or performance evaluations.	Yes	For the duration of your relationship with us plus any legal or regulatory retention period.
J. Non-Public Education Information	Education records directly related to a student maintained by an educational institution or party acting on its behalf, such as grades, transcripts, class lists, student schedules, student identification codes, student financial information, or student disciplinary records.	No	N/A
K. Inferences Drawn of the Consumer	Inferences drawn from Personal Information identified above to create a profile about a consumer reflecting a consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.	Yes	For the duration of your relationship with us plus any legal or regulatory retention period.

Category[1]	Examples	Collected	Retention Period
L. Sensitive Personal Information	Personal information that reveals (a) Social Security, driver's license, state identification card, or passport number; (b) account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credential allowing access to an account; (c) racial or ethnic origin, religious or philosophical beliefs, or union membership; (d) the contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication; or (e) genetic data. Biometric information processed for the purpose of uniquely identifying a consumer, personal information collected and analyzed concerning a consumer's health, sex life, or sexual orientation. Some Sensitive Personal Information included in this category may overlap with other categories. **Purposes for collection:** Processing and ongoing maintenance. **Is Your Information sold or shared?** No	Yes	For the duration of your relationship with us plus any legal or regulatory retention period.

Cookies and Tracking Technologies

Thrivent Bank uses cookies, web beacons, and similar tracking technologies on our website and mobile application to collect information about your browsing activity, improve your online experience, and for other purposes described below.

What are Cookies and Tracking Technologies?

- Cookies: Small text files that are placed on your computer or device by websites that you visit. They are widely used to make websites work, or work more efficiently, as well as to provide information to the website owners.
- Web Beacons: Small, transparent images embedded in web pages or emails that allow us to track whether a page or email has been viewed.

How We Use Cookies and Tracking Technologies

We use cookies and tracking technologies for the following purposes:

Types of Cookies	Purpose	Who Serves (for example)
Essential	These Cookies are required for the operation of the Services and enable you to move around the Services and use its features. Disabling these Cookies can negatively impact the performance of Services.	• Google • Adobe
Functionality	These Cookies are used to recognize you when you return to the Site. This enables us to personalize content for you and remember your preferences. These Cookies also enable your interactions with the Services such as emailing us.	• Google • Adobe • HubSpot
Analytics, Performance, and Research	These Cookies, beacons, and pixels allow us to analyze activities on the Services. They can be used to improve the functioning of the Services. For example, these Cookies recognize and count the number of visitors and see how they move around the Services. Analytics Cookies also help us measure the performance of our advertising campaigns to help us improve them and to optimize the content on the Services for those who engage with our advertising.	• Google • Adobe • Facebook • HubSpot
Social Networking	These Cookies are used to enable you to share pages and content that you find interesting on our Services through third-party social networking and other websites. These Cookies may also be used for advertising purposes.	• Google • Facebook
Advertising	These Cookies and pixels are used to deliver relevant ads, track ad campaign performance, or track email marketing.	• Google • Adobe

		• Facebook • HubSpot

Types of Cookies We Use

- Session Cookies: These cookies are temporary and expire when you close your browser.
- Persistent Cookies: These cookies remain on your device for a specified period, even after you close your browser.
- First-Party Cookies: These cookies are set by Thrivent Bank.
- Third-Party Cookies: These cookies are set by third-party service providers (e.g., analytics providers, advertising partners).

Managing Your Cookie Preferences

You have control over the use of cookies and tracking technologies. You can manage your preferences through the following methods:

- Browser Settings: Most web browsers allow you to control cookies through their settings. You can typically configure your browser to block all cookies, accept only first-party cookies, or notify you before accepting a cookie. However, please note that blocking essential cookies may affect the functionality of our Online Services.
- Cookie Consent Banner: When you first visit our website, you will be presented with a cookie consent banner that allows you to choose which types of cookies you accept. You can change your preferences at any time by accessing your cookie preferences directly from the website.
- Mobile App Settings: You can manage your mobile app tracking preferences through your device's settings.

How We Use Your Information

Thrivent Bank uses the information we collect, as described in the "Information We Collect" section above, for the following purposes:

Providing and Administering Financial Products and Services

We use your information to operate, maintain, and provide you with the features and functionality of our Online Services and to fulfill your requests for products and services. This includes:

- Processing your applications for accounts and loans.

- Opening, maintaining, and servicing your accounts.
- Processing transactions (deposits, withdrawals, transfers, bill payments, loan payments).
- Providing customer support and responding to your inquiries.
- Sending you important account-related notices and communications (e.g., statements, transaction confirmations, security alerts, legal notices).
- Administering your participation in programs.
- Fulfilling any other purpose for which you provide it.

Security and Fraud Prevention

We use your information to protect the security and integrity of our Online Services, our systems, and your accounts. This includes:

- Verifying your identity and authenticating your access to your accounts.
- Detecting, investigating, and preventing fraudulent transactions and activities.
- Monitoring for and responding to security threats and vulnerabilities.
- Protecting against unauthorized access, use, or disclosure of your information.

Legal and Regulatory Compliance

We use your information to comply with all applicable federal and state laws and regulations, including:

- Know Your Customer (“KYC”) requirements.
- Anti-Money Laundering (“AML”) regulations.
- Bank Secrecy Act (“BSA”) requirements.
- Office of Foreign Assets Control (“OFAC”) sanctions.
- Responding to legal process (e.g., subpoenas, court orders, search warrants).
- Cooperating with regulatory examinations and investigations.
- Reporting suspicious activities to the appropriate authorities.

Improving Our Services and Internal Operations

We may use your information to improve our Online Services, develop new products and features, and enhance the overall customer experience. This includes:

- Analyzing website and mobile app usage data to understand how our services are used and identify areas for improvement.
- Conducting internal research and analysis to develop new products and services.
- Testing and troubleshooting our systems and applications.
- Training our employees and improving our internal processes.

- Performing data analytics to understand customer needs and preferences. Where possible, we use aggregated or de-identified data for these purposes.

Marketing and Communications (Subject to Your Choices)

We may use your information to provide you with information about Thrivent Bank products, services, and promotions that may be of interest to you. This may include:

- Sending you marketing emails, direct mail, or other communications.
- Displaying targeted advertising to you on our website, mobile app, or on third-party websites and platforms.

You have the right to opt out of receiving marketing communications from us at any time. You can exercise this right by:

- Clicking the "unsubscribe" link in any marketing email you receive from us.
- Contacting us using the information provided in the "Contact Us" section of this Policy.
- Adjusting your communication preferences within your online banking account settings.

We will continue to send you service-related communications to you.

How We Share Your Information

Thrivent Bank understands the importance of protecting your personal information. We share your information only in limited circumstances, as described below, and always in accordance with applicable laws and regulations.

Internal Sharing

We may share your personal information within Thrivent Bank and with Thrivent Financial for Lutherans and its affiliates on a need-to-know basis for legitimate business purposes, consistent with this Policy and applicable law. This includes sharing for:

- Providing and administering the products and services you request.
- Managing your accounts.
- Processing transactions.
- Providing customer support.
- Complying with legal and regulatory requirements.
- Internal operations, research, and analytics (using aggregated or de-identified data whenever feasible).
- Fraud prevention and security.

- Marketing our products and services to you (subject to your opt-out rights, as described in the "Your Data Subject Rights" section).

Access to your personal information within Thrivent Bank and its affiliates is restricted to authorized personnel who have a business need to know the information.

Sharing with Service Providers

We may share your personal information with third-party service providers who perform services on our behalf and under our instructions. These service providers are contractually obligated to protect the confidentiality and security of your information and to use it only for the purposes for which it was disclosed. Examples of service providers and the types of information shared include:

- We share information necessary to provide core banking services, including account information, transaction data, and personal identifiers.
- We share information necessary to process your application, including your financial information, credit history, and personal identifiers.
- We share transaction information with payment processors to facilitate card payments and other financial transactions.
- We share information necessary to print checks for your account.
- We may share aggregated or de-identified data with analytics providers to improve our services.
- We may use cloud hosting providers to store and process your information. We ensure that these providers have appropriate security measures in place.
- We share information with fraud prevention services to verify your identity and protect against fraudulent activity.
- We may share information with marketing service providers to assist us in providing you with information about Thrivent Bank products and services.

Sharing with Affiliates

We may share your personal information with Thrivent Financial for Lutherans and its affiliates for operational purposes, such as risk management, compliance, and internal reporting.

We may share your personal information with Thrivent Financial for Lutherans and its affiliates for their own marketing purposes. You have the right to opt out of this sharing, as described in the 'Your Data Subject Rights' section below.

Legal and Regulatory Disclosures

We may disclose your personal information to government agencies, regulators, law enforcement, or other parties:

As required by law, such as in response to a subpoena, court order, or other legal process.

- To comply with regulatory reporting requirements (e.g., Suspicious Activity Reports ("SARs")).
- To cooperate with law enforcement investigations.
- To protect the rights, property, or safety of Thrivent Bank, our customers, or others.
- To enforce our agreements.

Thrivent Bank may disclose the information we collect about you, as listed above, with other parties. In addition to the specific situations discussed elsewhere in this policy, we disclose personal information to the following categories of other parties:

Categories Of Personal Information We Collect	To Whom We Disclose Personal Information for A Business Purpose
A. Identifiers – this may include real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number or other similar identifiers.	• Advertising networks • Data analytics providers • Government agencies or regulators may be needed to demonstrate our compliance with, or as required by, various laws and regulations or to prevent illegal activity. • Internet service providers • Operating systems and platforms • Payment processors and financial institutions • Professional services organizations, this may include auditors and law firms • Social networks • Other Service Providers
B. Additional categories of personal information described in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)) – this may include signature, physical characteristics or description, insurance policy number, bank account number, and other financial information.	• Government agencies or regulators may be needed to demonstrate our compliance with, or as required by, various laws and regulations or to prevent illegal activity. • Operating systems and platforms • Payment processors and financial institutions

Categories Of Personal Information We Collect	To Whom We Disclose Personal Information for A Business Purpose
	• Professional services organizations, this may include auditors and law firms • Other Service Providers
C. Characteristics of protected classifications – this may include age, citizenship, religion or creed and marital status.	• Government agencies or regulators as may be needed to demonstrate our compliance with, or as required by, various laws and regulations or to prevent illegal activity. • Operating systems and platforms • Professional services organizations, this may include auditors and law firms • Other Service Providers
F. Internet or other electronic network activity information – this may include browsing history, search history, and information regarding an individual's interaction with an internet website, application, or advertisement.	• Advertising networks • Data analytics providers • Government agencies or regulators may be needed to demonstrate our compliance with, or as required by, various laws and regulations or to prevent illegal activity. • Internet service providers • Operating systems and platforms • Professional services organizations, this may include auditors and law firms • Social networks • Other Service Providers
G. Geolocation data – such as IP addresses, which are registered to a geographical location.	• Government agencies or regulators may be needed to demonstrate our compliance with, or as required by, various laws and regulations or to prevent illegal activity. • Internet service providers • Operating systems and platforms

Categories Of Personal Information We Collect	To Whom We Disclose Personal Information for A Business Purpose
	• Professional services organizations, this may include auditors and law firms • Other Service Providers
H. Audio, electronic, visual or similar information – such as video, photos, or voice recordings.	• Advertising networks • Government agencies or regulators may be needed to demonstrate our compliance with, or as required by, various laws and regulations or to prevent illegal activity. • Internet service providers • Operating systems and platforms • Professional services organizations, this may include auditors and law firms • Other Service Providers
I. Professional or employment-related information – such as current or past job history.	• Government agencies or regulators may be needed to demonstrate our compliance with, or as required by, various laws and regulations or to prevent illegal activity. • Operating systems and platforms • Professional services organizations, this may include auditors and law firms • Other Service Providers
K. Inferences drawn from any of the information listed above – used to create a profile about you reflecting your preferences, trends or behaviors.	• Advertising networks • Data analytics providers • Operating systems and platforms • Other Service Providers
J. Sensitive personal information	• Government agencies or regulators may be needed to demonstrate our compliance with, or as required by, various laws and regulations or to prevent illegal activity.

Categories Of Personal Information We Collect	To Whom We Disclose Personal Information for A Business Purpose
	• Operating systems and platforms • Professional services organizations, this may include auditors and law firms • Other Service Providers

No Sale of Personal Information

Thrivent Bank does not sell your personal information for monetary consideration.

Your Data Subject Rights

Thrivent Bank is committed to respecting your privacy and providing you with choices regarding your personal information. Depending on your residency and the applicable laws, you may have the following rights. Please refer to your Privacy Notice to understand your eligibility for such rights:

Right to Know/Access

You have the right to request information about the categories and specific pieces of personal information we have collected about you, the sources of the information, the purposes for collecting it, and the categories of third parties with whom we share it.

You have the right to request a copy of your personal information in a portable and, to the extent technically feasible, readily usable format.

Right to Delete

You have the right to request that we delete your personal information, subject to certain exceptions permitted by law (e.g., we may need to retain information to complete a transaction, detect security incidents, comply with legal obligations, or exercise our legal rights).

Right to Correct

You have the right to request that we correct any inaccurate personal information we hold about you. If you believe that our information about you is incomplete, outdated, or incorrect, please contact us at (866) 226-5225.

You can also update your email address Online or in the Mobile App.

Right to Opt-Out of Sale/Sharing (CCPA/CPRA)

Thrivent Bank does not sell or share your personal information as defined under the CCPA, as amended by the CPRA. We do not disclose your personal information to third parties for cross-context behavioral advertising purposes.

Right to Non-Discrimination

We will not discriminate against you for exercising your privacy rights. This means we will not deny you goods or services, charge you different prices, or provide you with a different level or quality of goods or services solely because you exercised your rights under applicable privacy laws.

How to Exercise Your Rights

To exercise these rights or inquire about privacy protection at the Bank, visit our Privacy Web Form or call us at (855) 226-5225.

Please note that we may require additional information to verify your identity and process your request.

Verification Process

To protect your privacy and security, we will take reasonable steps to verify your identity before processing your request. This may involve asking you to provide information that matches the information we have on file, such as your name, address, account number, or other identifying details.

Response Timeframe

We will respond to your request within the timeframes required by applicable law. For example, under CCPA/CPRA, we generally have 45 days to respond to a verifiable consumer request, with a possible 45-day extension (with notice to you).

Authorized Agents (CCPA/CPRA)

If you are a California resident, you may designate an authorized agent to make requests on your behalf. We will require written proof of the agent's authorization and may also require you to verify your own identity directly with us.

Data Security

Thrivent Bank is committed to protecting the security of your personal information. We maintain a comprehensive information security program designed to safeguard your

data from unauthorized access, use, disclosure, alteration, or destruction. We use a combination of administrative, technical, and physical safeguards to achieve this.

Administrative Safeguards

- Information Security Policies and Procedures: We have established and maintain comprehensive written information security policies and procedures that comply with applicable laws and regulations.
- Employee Training: We provide regular data security and privacy training to all employees who have access to personal information. This training covers topics such as data handling, password security, phishing awareness, and incident response.
- Access Controls: We implement strict access controls to limit access to personal information to only those employees, contractors, and service providers who have a legitimate business need to know the information. Access is granted based on the principle of least privilege.
- Vendor Management: We carefully select and oversee our service providers who have access to personal information. We require them to maintain appropriate security measures and to comply with our privacy and security policies. We conduct due diligence and require contractual obligations related to data security.
- Incident Response Plan: We have a documented incident response plan in place to address any potential security breaches or incidents. This plan includes procedures for identifying, containing, investigating, and remediating security incidents, as well as notifying affected individuals and regulatory authorities as required by law.

Technical Safeguards

- Encryption: We use industry-standard encryption technologies, such as Transport Layer Security (“TLS”) and Advanced Encryption Standard (“AES”), to protect your personal information both in transit (when it's being transmitted between your device and our servers) and at rest (when it's stored on our systems).
- Firewalls: We use firewalls to protect our network and systems from unauthorized access.
- Intrusion Detection and Prevention Systems: We employ intrusion detection and prevention systems to monitor our network for suspicious activity and to block or mitigate potential threats.
- Vulnerability Scanning and Penetration Testing: We regularly conduct vulnerability scans and penetration tests to identify and address potential security weaknesses in our systems and applications.

- Multi-Factor Authentication (MFA): We offer and strongly encourage the use of multi-factor authentication for online banking access, adding an extra layer of security beyond just a username and password.
- Data Loss Prevention (“DLP”): We implement DLP measures to prevent sensitive data from leaving our controlled environment.
- Regular Security Audits: We conduct regular internal and external security audits to assess the effectiveness of our security controls.

Physical Safeguards

- Secure Facilities: We maintain physical security measures at our data centers and offices, including access controls, surveillance systems, and other safeguards to protect against unauthorized physical access to our systems and data.

Phishing Awareness

Thrivent Bank will never ask you to provide or confirm your personal information through an unsolicited email. Never respond to an email (especially unsolicited email) which asks for personal or account information. If you receive a suspicious email that appears to be from Thrivent Bank, please report it to us immediately using the contact information provided in the "Contact Us" section.

Your Role in Security

While we take significant measures to protect your information, you also play a crucial role in maintaining the security of your accounts and data. We encourage you to:

- Choose a Strong Password
- Protect Your Password
- Enable Multi-Factor Authentication
- Be Aware of Phishing
- Keep Your Software Updated
- Monitor Your Accounts

Children’s Privacy

Thrivent Bank is committed to protecting the privacy of children. Our Online Services (website and mobile applications) are not directed to children under the age of 13, and we do not knowingly collect personal information from children under 13 without verifiable parental consent, as required by the Children's Online Privacy Protection Act (“COPPA”).

If we become aware that we have inadvertently collected personal information from a child under 13 without verifiable parental consent, we will take immediate steps to delete that information from our systems.

If you are a parent or guardian and believe that your child under the age of 13 has provided us with personal information without your consent, please contact us immediately using the contact information provided in the "Contact Us" section of this Policy. We will work with you to address the situation and delete the information as required by law.

We encourage parents and guardians to supervise their children's online activities and to help them understand the importance of protecting their personal information.

Third-Party Links

Our Online Services (website and mobile applications) may contain links to websites or services that are not owned or controlled by Thrivent Bank. These third-party websites and services have their own privacy policies and practices, which may differ from ours.

We are not responsible for the privacy practices or the content of any third-party websites or services. When you leave our Online Services and navigate to a third-party website or service, we encourage you to read the privacy policy of that website or service before providing any personal information.

This Online Privacy Policy applies solely to information collected by Thrivent Bank through our Online Services. The inclusion of a link on our Online Services does not imply endorsement of the linked website or service by Thrivent Bank.

Changes to This Privacy Policy

Thrivent Bank may update this Online Privacy Policy from time to time to reflect changes in our practices, technology, legal requirements, and other factors. When we make changes, we will revise the "Last Updated" date at the top of this policy.

We encourage you to review this Policy periodically to stay informed about our privacy practices. Your continued use of our Online Services after any changes to this Policy constitutes your acceptance of those changes, to the extent permitted by law. If the changes made to this policy require action on the part of Thrivent, notice will be made on the website.

Contact Us

If you have any questions, concerns, or requests regarding this Online Privacy Policy or Thrivent Bank's privacy practices, please contact us using one of the following methods:

- By calling us toll-free at (866) 226-5225. Our call center is available Monday through Friday, 7 a.m. to 6p.m., Central Standard Time.
- Email: bank@thrivent.com
- You can also write us at:

  Thrivent Bank

  Attn: Compliance Department

  P.O. Box 71111

  Salt Lake City, UT 84121

For Data Subject Rights Requests (Access, Correction, Deletion, etc.)

Please refer to the "Your Data Subject Rights" section of this Policy for detailed instructions on how to exercise your rights. We encourage you to use our Privacy Web Form or for the most efficient processing of your request.