



Privacy Policy

Last updated: September 2025

We recognize that you trust us with your personal and financial information. This Privacy Policy explains how the U.S. Bancorp family of financial service providers (“we,” “us,” and “our”) may use and share information collected when customers, clients, and site visitors (“you” and “your”) visit or use our websites, mobile applications, and other online services to which a copy of this Privacy Policy is posted and including our branded social media pages (collectively, “our online services”). This Privacy Policy applies whether you visit or use our online services through your computer, smartphone, tablet, or other devices. It also explains your interactions with our advertisements, both with our online services and through our digital advertising campaigns.

Other privacy policies and privacy rights could also apply depending on how you interact with us, the financial products or services you may ultimately obtain from us, or the jurisdiction in which we are doing business with you. For example, one of our Consumer Privacy Policies would also apply to information that we collect about individuals who seek, apply for, or obtain our financial products and services for personal, family, or household purposes. While this Privacy Policy describes how we collect, use, and share information, please be aware that additional terms and conditions may apply for certain parts of our online services.

To the extent permitted by applicable law, by using our online services or otherwise interacting with one of our advertisements or accounts on a third-party site, you consent to this Privacy Policy, including our use and disclosure of information about you in the manner described in this Privacy Policy. To the extent permitted by applicable law, if you give any information about other individuals to us in connection with our online services, you represent that you have the authority to give to us such information and the authority to permit us to use such information in accordance with this Privacy Policy. Under certain circumstances, we may also obtain additional consents if required under applicable law.

This Privacy Policy explains:

1. [Information We Collect](#)
2. [How We Collect Information](#)
3. [How We Use Information](#)
4. [Why We Disclose Information/To Whom We Disclose Information](#)
5. [Online Tracking and Advertising](#)
6. [Linked Websites and Other Offerings](#)
7. [Data Security](#)
8. [Prevent Identity Theft](#)
9. [Children’s Online Privacy](#)
10. [External Aggregation Services](#)
11. [Social Media Platforms](#)
12. [Retention Periods](#)
13. [Cross-Border Transfer](#)
14. [State and International Laws](#)
15. [Changes to the Privacy Policy](#)

16. [Who We Are and How to Contact Us](#)
17. [Accessibility](#)

1. Information We Collect

We may collect personal information and other information about you, your device, your household, and your company. For example:

Identifying Information and Background

- Including name or alias, postal address, email address, and telephone number for your home or work
- Including your assigned customer number, employee identification number assigned to you by your employer, social media and proprietary platform IDs (e.g., RampIDs), or other assigned reference numbers and touchpoints
- Including education, employment, employment history, veteran or military status, and union membership
- Including account application information such as credit and income information or financial records

Government-Issued Identifiers

- Including Social Security number, driver's license and state identification card number, passport number, employer identification number (EIN), or other tax identification number (TIN)

Physical Characteristics and Demographic Data

- Including age or birthdate, marital status, parental status, physical characteristics or description, race, color, ancestry, national origin, citizenship, religion or creed, or sex (including gender, gender identity, gender expression, sexual orientation)
- Including your signature

Account Information and Payment Information

- Including account name and account number, security or access code, security questions and answers, password, or credentials allowing access to an account
- Including insurance policy number and other insurance information
- Including payment history, financial transactions, shopping history, and travel preferences

Location Data and Biometric Information

- Including physical location or movements, which may include your actual location to help you in finding a nearby ATM, branch, or office

We do not access location data stored on your device without your permission. Some features will not fully function unless you have enabled access to your location data.

- Including biometric information, for example, identify verification by voiceprint

We do not however have access to the information your device uses to enable facial or fingerprint recognition, nor do we have access to or store your facial image or fingerprint data. Your device may store the information it needs to recognize your facial features or fingerprints. Our online services may use your device's functionality to obtain a signal that your device recognizes your facial features or fingerprints when you sign on. You can always turn off facial or fingerprint recognition and go back to inputting user ID and password at any time. Your device's user information will have additional information about its user controls and settings, including its privacy and security controls.

Company and Commercial Information

- Including formation and organization documents, information about owners and employees, and financial records
- Including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies
- Including billing address, business contact information, travel preferences, and specific expenses

Audio and Visual Information

- Including documents or images submitted via our online services, such as selfies, checks, and banking statements
- Including audio and visual information, including audio, electronic, or similar information we capture through your communications with us (for example, voice recordings of telephone conversations, emails and instant messaging, and security images if you visit our branches or offices)
- Including photographs, images, videos, and recordings of your voice (such as when we record customer service calls for quality assurance and training purposes)

Device Information and Other Unique Identifiers

- Including unique personal identifier, online identifier, Internet Protocol address, hashed email address, hashed telephone number, mobile advertising IDs (MAID) (e.g., Android Advertising ID (AAID), Google Advertising ID (GAID), Google Click ID (GCLID), and Apple's identifier for advertisers (IDFA)), or other identifiers
- Including the type of operating system and browser you use, the parts of our online service you access, your Media Access Control (MAC) address and other device identifiers, computer type (Windows® or Macintosh®), screen resolution, operating system name and version, device manufacturer and model, language preferences, Internet browser type and version

Internet or Other Network Activity

- Including data resulting from your activity, such as transaction information and the pages you visit on our online services, social media preferences, and log information such as your search and voice to text queries in the mobile app, Internet, or other electronic network activity information, including browsing history and the sites you visit, referring URLs, search history, information on you or your device's interaction with our online services or other websites, applications, or advertisements
- Including whether you received, accessed, or acted in response to the contents of your mail, email, text messages, and calendar invites that we send to you (or that others send on our behalf) or that you send to us
- Including responses to advertisements on sites and mobile apps where we advertise
- Including behavioral characteristics, such as keystroke and mouse movement patterns

Attitudinal Data and Inferences

- Including attitudinal data from consumer satisfaction surveys, voice inflection, product desirability, and purchase criteria
- Including inferences drawn from other personal information to create a profile about you reflecting preferences, characteristics, attitudes, and/or similar trends (for example, we may later associate the usage and other information we and our ad partners collect online with personal information about you, your household, your device, your company, or others)

Additional Information

- Including information to help virtual or in-person event management (for example, attendee names, dietary requirements, special assistance needs, and travel details for participants)

- Including information collected when providing your business card or other contact information during business meetings, at trade shows, or other in person events
- Including information about you from other online and offline sources, such as co-branded partner sites, public databases, social media platforms, data brokers, credit reporting agencies, identity verification services, aggregators, and other third parties

Analytics Information and De-identified Data

- Including analytics data that we may directly or indirectly collect, including with the use of third-party analytics tools such as Google Analytics® to help us measure traffic and usage trends for our online services and to understand more about the demographics of our users

You can learn more about Google’s practices at:

<http://www.google.com/policies/privacy/partners> and view its opt-out options at <https://tools.google.com/dlpage/gaoptout>

- Including de-identified data

We also maintain and use de-identified data for some purposes in such a way that any information can no longer be linked to you or any device associated with you. When using de-identified data, we take reasonable measures to ensure that the information cannot be reassociated with you or your device. We have also implemented technical and organizational safeguards as well as business processes designed to prohibit the reidentification of your information. We contractually obligate recipients of the de-identified data to comply with applicable laws about deidentification and we monitor compliance with any contractual commitments in accordance with our vendor due diligence programs. In certain limited circumstances, we may reidentify such data for the purposes of providing the online services and customized recommendations. In such circumstances, our use of such personal information is in accordance with our privacy commitments under applicable privacy policies.

2. How We Collect Information

We collect information from various sources. For example:

From You

We collect information from you or about you when you provide this information to us directly. For example, we may obtain information when you apply for or obtain products or services from us, engage our online services (including when using co-browsing, if available), respond to surveys, contact customer support or our call centers, engage in chat features through our online services, visit our branches or offices, or otherwise interact with us.

From Your Employer or Your Company

If you interact with us through your employer or company, we may receive your information from your employer or company, including from another representative of your employer or company.

From Tracking Technologies

We, and our third-party partners, may automatically collect (intercept, record, maintain, share, disclose) information about your activity when you are using our online services, receiving emails, or otherwise engaging with us. We typically collect this information through a variety of tracking technologies, including (i) cookies or small data files that are stored on your computer or other device, (ii) the use of session replay tools or data collected through the deployment of video content, and (iii) other related technologies, such as web beacons, pixels, embedded scripts, mobile SDKs, location-identifying technologies, and logging technologies (collectively, “tracking technologies”) and we may use third-party partners or technologies to collect this information. Information we collect automatically about you may be combined with other information we collect directly from you or receive from other sources. Please go to [Online Tracking and Advertising](#) below for more information.

From Other Online and Offline Sources

We may also receive information about you from other online and offline sources, such as public databases, social media platforms, and other third parties. For example, we collect information when you use aggregation services to consolidate your financial information or respond to us or we otherwise reach out to you for marketing or other purposes. We may also obtain information about you from other sources, such as data analytics providers, marketing or advertising service providers, social media platforms, aggregators, fraud prevention service providers, vendors that provide services on our behalf, or publicly available sources.

From Models, Predictions, and Profiles

We also create information, models, predictions, and profiles about you, your household, your company, and others based on our analysis of the information we have collected from and about you and others.

3. How We Use Information

We may use the information to:

Offer and deliver products and services to you

- Operate, evaluate, and improve our business (including improving existing and developing new products and services for us, our affiliates, or our partners)
- Perform accounting, auditing, and other internal business operations
- Respond to requests, communicate with you, provide customer support, resolve disputes, and manage your preferences

- Personalize your online experience and allow you to use features within our online services, including autocompleting applications
- Provide advertising to you, your company, and others (including others like you)
- Detect and prevent fraud and enhance the security of our business, your accounts, or our online services
- Help evaluate bias and improve credit risk management
- Verify your identity or location for security, fraud prevention, and other risk control purposes
- Conduct and publish aggregated research, industry indicators, and benchmarking
- Perform data analytics
- Comply with and enforce applicable legal requirements, relevant industry standards, contractual obligations, and our policies and otherwise protect our rights and operations
- For any other purposes permitted by applicable law
- For any other purposes that we may specifically disclose at the time that we collect your information

We may use artificial intelligence (AI), generative AI, predictive models, or machine learning, including third-party external consumer data and information sources, in compliance with applicable laws and regulations, to improve, promote, and deliver products and services and augment our business practices.

4. Why We Disclose Information/ To Whom We Disclose Information

We may disclose information in different ways and to different persons as permitted or required by law. For example, we may disclose or share information:

- To process transactions requested by you
- To effect, administer, or enforce a transaction
- With your consent
- To protect the confidentiality of records, to protect against fraud, to resolve customer disputes
- To provide information to insurance rate advisory organizations, rating agencies, persons assessing our compliance with industry standards or our attorneys, accountants, and internal and external auditors
- To comply with contractual and legal obligations and requirements
- To a consumer reporting agency (credit bureau)
- In connection with a proposed or actual sale or merger of all or part of our business, business line, portfolio, or portion of our business
- With our vendors, service providers, and other third parties
- With our affiliates and otherwise within the U.S. Bancorp family of financial service providers
- With law enforcement, regulatory and other governmental agencies, and other third parties to comply with relevant laws and regulations and properly authorized subpoenas or with other official agencies with authority over us, such as regulatory agencies
- With other companies to joint market or to bring you co-branded services, products, or programs
- To persons holding a beneficial interest relating to you or persons acting on behalf of you
- For any other lawful purpose or as otherwise required by applicable law

We may use and disclose information even when you are no longer our customer or client.

5. Online Tracking and Advertising

We recognize Global Privacy Control (GPC), which is a setting that allows you to communicate your privacy preferences to websites and online services that you visit. When we detect a GPC signal from a browser, our online services are designed to treat the browser as opted out and to stop sharing personal information for certain targeted advertising purposes, in accordance with applicable laws. Please visit the [Global Privacy Control](#) website to learn more about the setting and how to enable it on your browser.

You can also opt out of certain targeted advertising by visiting [YourAdChoices.com](#) and by adjusting the privacy settings on your mobile device (e.g., “Limit Ad Tracking” on iOS or “Opt out of Ads Personalization” on Android). You may be able to set your web browser to tell you when cookies are set, delete your cookies, or block cookies altogether. Please check your browser’s settings or support pages to learn how to manage cookies and other tracking technologies on your browser or device.

We use advertising platforms, The Trade Desk and LiveRamp, to help us execute our marketing campaigns. These third parties may also provide you with the ability to further limit the use and sharing of your information for advertising purposes with their other clients. You may visit The Trade Desk at <https://adsrvr.org/> and LiveRamp at <https://liveramp.com/privacy/> to learn more about their privacy practices and opt-out options.

Please note that your preferences will apply only to the specific browser or device from which you opt out. You will need to opt out separately on all your browsers and devices. If you delete cookies, change web browsers, reset your mobile advertising ID, or use a different device, you may need to opt out again. **If you choose to reject cookies, some features of our online services (including account access to our digital services) may no longer function. Please see your *Digital Services Agreement* with us for details.**

Please note that even if you opt out, you may still receive online advertising from us. Opting out from a specific advertising provider means that the ads you do receive will not be based on your preferences or behavior. In addition, you may still see targeted pages based on your habits as you navigate our online services, including www.usbank.com.

You may have additional rights to opt out of our use of your information depending on how you interact with us, the financial products or services you may ultimately obtain from us, or the jurisdiction in which we are doing business with you. For example, if you do not want us to serve you targeted advertising based on your visit to our online services, you can opt out of targeted advertising by selecting [Your privacy choices](#).

6. Linked Websites and Other Offerings

Our online services may have links to third-party websites, widgets, plug-ins, applications, or offerings not controlled by us. We encourage you to be aware when you leave our online services and to read the privacy policies and terms of use of any such websites or offerings that may collect your information, as they will likely differ from those of our online services. We do not guarantee, and we are not responsible for the privacy or security of these websites or

offerings, including the accuracy, completeness, or reliability of their information or data practices.

For example, we may disclose your information to advertising platforms at your direction, or security service providers to help prevent unauthorized access to our online services. Please be aware that these parties' privacy notices apply to the information that you share directly with them. For example, we use Google's reCAPTCHA to prevent misuse of our online services.

In addition, we are not responsible for the information collection, use, and disclosure practices (including the data security practices) of other organizations, such as Meta®, Instagram®, and X®, or any other app developer or provider, social media platform provider, operating system provider, wireless service provider, or device manufacturer.

7. Data Security

We will use reasonable organizational, physical, technical, and administrative measures to protect personal information within our organization. Unfortunately, no data transmission or storage system can be guaranteed to be 100% secure. If you have reason to believe that your interaction with us is no longer secure, please immediately notify our [Fraud Department](#).

8. Prevent Identity Theft

To help us protect your personal information, it is important that you always keep your account information safe. Do not share your username, password, or PIN with anyone.

We will never initiate (unless otherwise stated for a specific product or service application), a request via email for your sensitive information (for example, Social Security number, username, password, PIN or account number). If you receive an email asking for your sensitive information, you should be suspicious of the request and promptly contact us to report the suspicious activity.

Please be aware, however, that in certain telephone and in-person transactions we may ask for your full Social Security number, account number or other information to verify your identity before conducting the transactions you have requested. For example, we may ask for such information to verify your identity when you place a call to us, when you visit a U.S. Bank branch office or when we call you about a new product or service, we believe that you will find valuable. We will never request that you disclose your personal ID, password or PIN under any circumstances, including such telephone or in-person transactions.

Additional information regarding how to protect yourself from financial fraud can be found at [Security](#).

9. Children's Online Privacy

We do not use our online services to knowingly solicit personal information from or market to children under the age of 13 without parental consent. We request that such individuals do not provide personal information through our online services. If parents or guardians becomes

aware that their child has provided us with information without their consent, they should promptly contact us in accordance with the [Who We Are and How to Contact Us](#) section below and we will delete such information from our files.

10. External Aggregation Services

Some companies offer financial management tools that allow you to access account information (including account statements and tax documents) from a variety of sources so that you can view multiple accounts at a single online location. These services may require you to provide personal identification information, including specific account information and your log-in credentials. By providing your log-in credentials to such a service you authorize that service to access your account which may include the ability to initiate transfers to or from your account. Please use caution when providing personal information and log-in credentials to third party service providers and read and understand the third party's privacy and security policies before sharing any personal information with the service. Any use of a third-party site is at your own risk. If you elect to provide your log-in credentials or other information about your accounts to a third party, you are responsible for the use of your account or the disclosure of any personal information by the third party. Should you decide to revoke any access you have given to a third party, you must contact us, in which case we may need to block your access to our digital services until we issue new log-in credentials.

11. Social Media Platforms

We may interact with users of various social media platforms, including Meta[®], Instagram[®], X[®] and LinkedIn[®]. Please note that any content you post to such social media platforms (for example, pictures, information, or opinions), as well as any personal information that you otherwise make available to users (for example, your profile), is subject to the applicable social media platform's terms of use and privacy policies. We recommend that you review this information carefully to better understand your rights and obligations with regard to such content.

12. Retention Periods

We store information for as long as necessary to carry out the purposes for which we originally collected it and for other legitimate business purposes, including to meet our legal, regulatory, or other compliance obligations.

13. Cross-Border Transfer

The online services linking to this Privacy Policy are controlled and operated by us from the United States. We have service providers in the United States and other countries. Therefore, we and our service providers may transfer your personal information to, or store or process your information in any country where we have facilities or in which we engage service providers, including in jurisdictions that may have different data protection rules than those of your country. We will take steps to ensure that your personal information receives an adequate level of protection in the jurisdictions in which we process it.

For non-U.S. online services, please review the privacy policy applicable to that service to understand how your information will be collected, processed, and safeguarded.

14. State and International Laws

In addition to the federal laws concerning the collection and use of personal information that apply to financial institutions, additional privacy rights may be applicable based on your local jurisdiction. For example, for information regarding California's privacy laws and the procedures that we have in place to comply, please go to the [California Privacy Center](#) page.

15. Changes to the Privacy Policy

From time to time, we may update this Privacy Policy to accommodate new technologies, industry practices, regulatory requirements, or for other purposes. We encourage you to review this Privacy Policy periodically to ensure that you understand what we collect and how we use and share information through the online services. If we do update this Privacy Policy, we will let you know by posting the revised policy with a new **"Last updated"** date posted at the top of this policy. We may also provide you with an additional notice (such as by adding a statement to our online services or sending you a notification), in connection with making material changes to this Privacy Policy. We encourage you to review this Privacy Policy regularly to stay informed about our information practices and the choices available to you.

Any changes to this Privacy Policy will become effective when the revised policy is posted (and subject to any advance notice that may be required under applicable law). By continuing to use the online services following such changes, you are agreeing to accept the terms of the revised Privacy Policy.

16. Who We Are and How to Contact Us

This applies to the U.S. Bancorp family of financial service providers.

If you have any questions or comments about this Privacy Policy or our privacy practices generally, we encourage you to contact our customer service department by calling 800-872-2657 or use the Contact Us methods listed below.

17. Accessibility

If you need this information in an alternate accessible format, call us at 800-872-2657. We accept relay calls. Please see our [Accessibility at U.S. Bank](#) page for more information.