

# Online Privacy Policy

**At Sovereign Bank, “we,” “us” or “our” trust has always been the foundation of our relationship with customers. We understand your desire for privacy, and we recognize that you trust us with your personal and financial information. Our Online Privacy Policy is designed to describe our privacy practices and principles in a format that is easy to navigate, read and understand. We will treat your personal information with the utmost care and respect.**

## Online Privacy Policy

This Online Privacy Policy (the "Policy") describes the treatment of information that is provided or collected through any of our online interfaces to which a copy of the Policy is posted, including [www.banksovereign.com](http://www.banksovereign.com) (the "Website"), Applications we have placed on third party sites such as Facebook®, Twitter® and other social media services, and Sovereign Bank's mobile applications (the "Applications," and together with the Website, the "Services"). It also explains how we collect, use and share information based on users' interactions with online advertisements, both on the Services and on online interfaces owned by third parties. Note that the Policy does not govern our privacy practices offline or with respect to information that is not provided or collected through the Services. We will use and share any information that we collect from or about our customers in accordance with the Sovereign Bank Privacy Policy, which provides choices regarding our sharing and use of information. For additional information on this Policy or our privacy practices generally, please refer to the "Disclosures" portion of the Website or feel free to contact us with your questions.

While this Online Privacy Policy describes how we treat information, please be aware that additional terms and conditions may apply for certain parts of our Website and Applications.

## 1. Types of Information We Collect

We collect two basic types of information through the Services – personal information and anonymous information. We also collect location information in connection with certain of our mobile applications.

"Personal information" refers to information that identifies (whether directly or indirectly) a particular individual, such as information you provide on our forms, surveys, applications or similar online fields. Examples may include your name, postal address, email address, telephone number, Social Security number, date of birth or account information.

"Anonymous information" means information that does not directly or indirectly identify, and cannot reasonably be used to identify, a particular individual. Examples may include information about your Internet browser, information collected through tracking technologies, demographic information that you provide to us (e.g., your household income) and aggregated or de-identified data.

"Location information" means information that may be collected by certain mobile applications that identifies your physical location.

We also collect location information in connection with certain of our mobile applications.

## 2. How We Collect Your Information

We collect personal information from you or about you when you provide this information to us directly. For example, we may obtain personal information when you request information, products or services from us, register on the Website or an Application, respond to surveys, contact customer support or otherwise interact with us. We may also receive information about you from other online and offline sources, such as public databases, social media platforms and other third parties.

In addition, we may collect information about your activity on the Services automatically using tracking technologies, such as cookies, Flash cookies and pixel tags. If you submit any personal information relating to other people to us or to our service providers in connection with the Services, you represent that you have the authority to do so and to permit us to use the information in accordance with this Policy.

## 3. How We Use Information That We Collect

We may use information that we collect in order to, among other things:

- Provide you with, or evaluate your eligibility for, products and services that you request from us
- Communicate with you about your accounts or transactions with us
- Send you important information regarding the Services, changes to this Policy and/or other similar administrative information
- Allow you to participate in surveys, sweepstakes, contests and similar promotions, and to administer such promotions (note that these promotions may contain additional disclosures regarding our collection and/or use of your information)
- Consistent with local law, required disclosures, and choices and controls that may be available to you:
- Send you offers and promotions for our products and services, or products and services that may be of interest to you;
- Personalize content and experiences on the Services;
- Verify your identity and/or location (or the identity or location of your authorized representative) for security, fraud prevention and other risk control purposes
- Provide you with advertising based on your activity on the Services and on third-party websites and applications.
- Optimize or improve our products and services
- Detect, investigate and prevent activities that may violate our policies or be illegal
- Comply with our legal and regulatory obligations
- Enforce our terms and conditions and otherwise protect our rights and operations

#### 4. How We Share Information That We Collect

We will not share your personal information outside the Sovereign Bank family of financial service providers, except under limited circumstances. Please refer to the Sovereign Bank Privacy Policy for additional information regarding how we may share personal information, as well as the choices you may be able to exercise in connection with such sharing.

#### 5. Online Tracking and Advertising

We and certain trusted service providers operating on our behalf collect information about your activity on the Services using tracking technologies, including:

- **Cookies** are pieces of information that are stored directly on the device that you are using. They allow us to collect information such as the type of browser you are using, the amount of time you spend using the Services, the websites or applications you visit and the preferences you have set up for your accounts. We use this information for such purposes as to personalize your experience, enhance security, facilitate navigation, display material more efficiently, recognize the device that you are using to access the Services and understand how the Services are used. The Services do not use cookies that capture unencrypted personal information about you.

You can choose to have your device refuse to accept any cookies, and the majority of devices and browsers offer additional privacy settings for cookies. You do this through your browser settings. Each device and each browser is a little different, so look at your device Settings or your browser Help menu to learn the correct way to modify your cookies. If you turn cookies off, you will not have access to many features that make your user experience more efficient and some of the Services will not function properly. Please note that you will need to manage your cookie settings for each device and browser that you use.

- **Pixel tags, web beacons, clear GIFs and other similar technologies.** These are typically small pieces of data that are embedded in images on the Website, our Applications or certain e-mail communications. They may involve the transmission of information directly to us, to another party on our behalf or to another party in accordance with its privacy policy. We may use these technologies to bring together information we collect about you.
- **Location tracking on mobile devices.** Certain applications on mobile devices may transmit information to us about your location when you request information from them. An example includes your physical location when you search for a nearby ATM using your mobile device. We may use that information to improve the products and services we provide to you as well as improving our services generally in your area. Information collected through tracking technologies is used for many purposes including, for example, to:
  - Provide useful features to simplify your experience when you return to the Services
  - Deliver relevant content based on your preferences, usage patterns and location
  - Monitor and evaluate the use and operation of the Services
  - Analyze traffic on the Services and on websites or mobile applications of third parties
  - We may associate this tracking data with your registration information, in which case we will treat it as personal information.

We use Google Analytics, which uses cookies and other, similar technologies to collect information about use of the Services anonymously and reports website trends, without identifying individual visitors. To learn more, including how to opt out, visit <https://tools.google.com/dlpage/gaoptout>.

Occasionally, you may encounter banner advertisements for our products and services on third-party websites and mobile applications. We use third-party advertising service providers to distribute our advertisements on websites and mobile applications where we have paid to advertise. These advertisements may use tracking technologies to capture information such as IP address, browser type and usage information in order to track the effectiveness of our advertising efforts. Such tracking technologies do not capture personal information about you, and our advertising service providers are prohibited from using any information collected except to track advertising effectiveness.

In addition, we use advertising service providers such as Google, Yahoo and MSN to place advertisements for our accounts and services on websites not affiliated with us, and to help us determine which of our advertisements are most likely to be of interest to you using non-personal behavioral information. Advertisements placed by these service providers may use tracking technologies that allow monitoring of your responsiveness to such advertisements. We restrict access and collection of information by advertising service providers for purposes other than assisting us with our advertising efforts.

In order for behavioral advertising opt-outs to work on your device, your browser must be set to accept cookies. If you delete cookies, buy a new device, access the Services from a different device, log-in under a different screen name or change web browsers, you will need to opt-out again. If your browser has scripting disabled, you do not need to opt-out, as online behavioral advertising technology does not work when scripting is disabled. Please check your browser's security settings to validate whether scripting is active or disabled.

## 6. Other Information Collected Automatically

**Browser or Device Information:** Certain information is collected by most browsers or automatically through your device, such as your Media Access Control (MAC) address, computer type (Windows or Macintosh), screen resolution, operating system name and version, device manufacturer and model, language, Internet browser type and version, and the name and version of the Services (such as the Application) you are using. We use this information to ensure that the Services function properly.

**Application Information:** When you download and use an Application, we and our service providers may track and collect usage data, such as the date and time the Application on your device accesses our servers and what information and files have been downloaded to the Application based on your device number.

**IP Address:** Your IP address is a number that is automatically assigned to your computer by your Internet Service Provider. An IP address may be identified and logged automatically in our server log files whenever a user accesses the Services, along with the time of the visit and the page(s) visited. Collecting IP addresses is standard practice and is done automatically by many websites, applications and other services. We use IP addresses for purposes such as calculating usage levels, helping diagnose server problems and administering the Services.

## 7. Linked Websites

The Services may contain links to third-party websites not controlled by Sovereign Bank. We encourage you to be aware when you leave the Services and to read the privacy policies and terms of use of any such websites that may collect your personal information, as they will likely differ from those of the Services. Sovereign Bank does not guarantee and is not responsible for the privacy or security of these websites, including the accuracy, completeness or reliability of their information.

In addition, Sovereign Bank is not responsible for the information collection, use and disclosure practices (including the data security practices) of other organizations, such as Facebook, Apple, Google, Microsoft, RIM or any other app developer or provider, social media platform provider, operating system provider, wireless service provider or device manufacturer.

## 8. Data Security and Online Risk-Free Guarantee

Your privacy is very important to Sovereign Bank and we are committed to protecting your personal information from unauthorized access or use. We seek to 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 us in accordance with the “Contact Us” section below.

In addition, Sovereign Bank protects customers from liability for unauthorized online transactions. We will protect you from unauthorized transfers to or from your consumer accounts (those used for personal, family or household reasons) that are initiated via banksovereign.com, by using our mobile app, or by using our online bill pay service. Sovereign Bank will cover 100% of any losses from unauthorized online transactions, so long as they are reported to us promptly and you have not provided access to your accounts to others. You must protect your passwords to ensure that there are no unauthorized users accessing your account(s). Report to us, within 60 days of the first statement date when the unauthorized transactions appear.

You have the responsibility to help us protect your accounts by never revealing your username or password to other individuals. These protections are subject to certain restrictions, and may not apply to commercial and small business accounts.

## 9. Preventing Identity Theft

In order to help us protect your personal information, it is important that you always keep your account information safe. Never share your personal ID, password or PIN with anyone, under any circumstances.

Note that Sovereign Bank will never initiate a request via email for your sensitive information (e.g., Social Security number, personal ID, 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 Sovereign 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 identity theft and the steps you can take to help protect yourself from fraud can be found on the Federal Trade Commission website.

## 10. Children's Privacy

We do not use the Services to knowingly solicit personal information from or market to children under the age of thirteen (13) without parental consent. We request that such individuals do not provide personal information through the Services.

If a parent or guardian becomes aware that his or her child has provided us with information without their consent, he or she should promptly contact us and we will delete such information from our files. For additional information regarding the Children's Online Privacy Protection Act (COPPA), please visit the Federal Trade Commission website ([Opens in a new Window](#)).

## 11. External Aggregation Services

Some third-party companies offer aggregation services that allow you to consolidate your financial account information from a variety of sources, such that you can view all your account information at a single online location. For example, an aggregation service might collect and consolidate your checking and savings account balances at your bank, the value of your stocks and bonds in your brokerage account and your frequent flier mileage information from an airline. In order to do so, the aggregator may request access to personal information - including identification information, account information, personal IDs and passwords - from you for each individual website. You must provide your permission and access to your personal information to allow these services to collect this data.

Please use caution when providing personal information to aggregation services. You should always ensure that the aggregator has appropriate policies and practices in place to protect the privacy and security of any personal information to which the company is gaining access. Sovereign Bank is not responsible for the use or disclosure of any personal information accessed by a company or an individual to whom you provide the personal ID and password required to access your accounts through the Services.

If you do elect to provide your personal ID, password or other information about your accounts with us to an aggregation service, you will be unable to contest the validity of any Sovereign Bank transaction initiated by the aggregator, whether or not you were aware of the specific transaction. Should you decide to revoke the authority you have given to an aggregation service, you may only do so by contacting us, in which case we may need to block your account until we issue new access codes.

## 12. Social Media Platforms

Sovereign Bank may interact with registered users of various social media platforms, including Facebook® and Twitter®. Please note that any content you post to such social media platforms (e.g., pictures, information or opinions), as well as any personal information that you otherwise make available to users (e.g., 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 in order to better understand your rights and obligations with regard to such content.

## 13. Updating Your Information

It is very important that you keep the information associated with your account accurate and up-to-date. If you believe that your account information is incomplete, inaccurate or otherwise not current, please contact us and provide us with the appropriate information. Alternatively, you may call or write to us at the telephone numbers or appropriate address for changes listed on your account statements, records, online or other account materials.

If you would like to review, correct, update, suppress or delete personal information that you have previously provided to us, you may contact us.

In your request, please make clear what personal information you would like to have changed, whether you would like to have it suppressed from our database or otherwise let us know what limitations you would like to put on our use of the personal information you have provided to us. For your protection, we may only implement requests with respect to the personal information associated with the particular email address that you use to send us your request, and we may need to verify your identity before implementing your request. We will try to comply with your request as soon as reasonably practicable.

Please note that we may need to retain certain information for recordkeeping purposes and/or to complete any transactions that you began prior to requesting a change or deletion. There may also be residual information that will remain within our databases and other records, which will not be removed.

#### **14. Retention Period**

We will retain your personal information for the period necessary to fulfill the purposes outlined in this Policy, unless a longer retention period is required or permitted by law.

#### **15. Cross-Border Transfer**

The Services are controlled and operated by us from the United States, and are not intended to subject us to the laws or jurisdiction of any state, country or territory other than that of the United States. We may store and process your personal information in any country where we have facilities or in which we engage service providers, and, by using the Services, you consent to the transfer of information to countries outside of your country of residence, including the United States, which may have different data protection rules than those of your country.

#### **16. Changes to the Online Privacy Policy**

From time to time, we may make changes to this Policy in order to accommodate new technologies, industry practices, regulatory requirements or for other purposes. We encourage you to review the Policy periodically to ensure that you understand how we collect, use and share information through the Services. If we do make changes to the Policy, we will also update the "Effective Date" posted at the top of the Policy.

Any changes to the Policy will become effective when the revised Policy is posted on the Website, relevant Application or other Sovereign Bank online interface, as applicable. By continuing to use the Services following such changes, you are agreeing to accept the terms of the revised Policy.

### **Contact Us**

If you have any questions or comments about this Policy or our privacy practices generally, we encourage you to contact our customer service department by completing our online email form or by calling 833.782.6500

Alternatively, you may use any of the local telephone numbers for your area that are listed in the "Contact Us" section of the Customer Service portion of the Website.

In the event you notice suspicious activity on your account or believe your personal ID, password or PIN has been compromised, please contact us immediately. Suspicious emails may be forwarded to [info@banksovereign.com](mailto:info@banksovereign.com) or you can call us at **833.782.6500**