MOBILE PRIVACY DISCLOSURE

Rev. 02/2022

FACTS	What does TEXAS NATIONAL BANK Do with your personal information from the Mobile applications?
Why?	This **Mobile Privacy Notice** describes how our Mobile Banking Applications ("Mobile Apps") collect and use information about you when you interact with us online through our Mobile Apps with the use of your personal smartphones, tablets, or other mobile devises. When visiting and using any of our Mobile App, the applications may require the access to information stored on your mobile device required to be able to provide you these online products and services in a safe and secured manner. By subscribing, accessing, and using any of our Mobile Apps, products, and services on our website or directly through our Mobile Apps, you agree to the terms and conditions of this privacy policy. It is important for you to understand that: • Before granting access to this information, you will be prompted to give the application that permission (consent). • If you do not wish to grant that permission, you may decline. • If you later change your mind, those permissions can be updated in your device's settings. • Your mobile device setting may also be set to share the information only when the app has been activated and in use.
What?	**Types of information our Mobile Apps will access** and require will depend on how you interact and use our App's, and may include: **Information Collected directly from you:** • Your personal identifying Information - required to identify you as a bank customer and approve your access to our Mobile Apps. • User Authentication information -required to identify and grant your access as an authorized user when signing on to our Mobile Apps. • Account Information - required to view your account activity, or process transactions you initiate when using our Mobile Apps. **Information Collected / Accessed from your mobile devices:** • Contacts - is access when using "People Pay" (Person-to-Person Payment Services) available via our Mobile Apps, which is used to create a payee when you elect to use the app. • Geo-Location Information - is access to provide location-based services by identify your location within our service areas to provide you the location of our branches and ATMS's near to you. • Camera - Access is required and used for Biometric Face or Fingerprint Recognition, as part of an authentication process to identify you as an authorized user, to capture images of ID's when submitting a loan application, or images of checks when using our remote deposit option and/or to share images of other information we may request from you. • Your mobile device ID Information (IP Address) - used to authenticate and grant access of users to our Mobile Apps (This includes browser type. Location of device, devise ID/IP Address, operating system, and mobile network information). • Cookie & Web Beacons – We may use cookie, web beacons, tracking pixels and tracking technologies on some of our Mobile Apps to help customize the application, and improve your experience and the performance of our Site by, among other things, allowing us to monitor Site performance, making the Site easier to use, and measuring its effectiveness. The cookies and web beacons we use collect non-personally identifiable information about users of the Site.

MOBILE PRIVACY DISCLOSURE

Rev. 02/2022

How?

How do we use your personal information?

We are committed to transparency about how we use your personal information, and we ask for your consent when required, otherwise by using our Site and Mobile Apps, you consent to the collection, use and sharing of your personal information subject to applicable laws and regulations.

Personal information collected from and about you as described in the Notice may be used for many purposes such as:

- Delivering our Mobile Apps products and services in a safe and secured manner.
- To approve and grant your access to our Mobile Apps.
- Personalizing your digital and mobile banking experience by providing relevant alerts, products, and services, like finding nearby ATMs, and branch locations.
- Detecting and Preventing Fraud
- Complying with and enforcing applicable legal requirements, industry standards, contractual obligations, and in accordance with our security policies.
- Providing you network notifications and security alerts.
- Providing a secure and effective means of communicating and sharing information with you.

How may we share your personal Information?

We may share your information we collect from and about you online consistent with this Notice subject to other legal and regulatory restrictions such as:

- With third-party providers to process your personal information for business purposes on our behalf. These third-party providers are contractually obligated to comply with our policies to protect information we share with them, and/or they collect on our behalf.
- To comply and respond to governmental inquires, court orders and subpoenas.
- To protect the rights, privacy, safety, and property of Texas National Bank.
- To permit us to purse available remedies or losses sustained resulting form the inappropriate use of our sites and customers information.

Information Security?

Protecting your personal information

To protect your personal information from unauthorized access and use, we use administrative, technical, and physical security measures that comply with federal laws and regulations. These measures include computer safeguards, secured files and buildings.

Record Retention

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

Limiting and Sharing of Information

If you choose to decline, and/or block access to some information from your mobile devise, like "Cookies" by changing the security settings on your mobile devise, or internet browser. Please note this may disable or limit some of the functionalities of the Mobile Apps rendering it unusable, which may result in your inability to successfully log onto to or use our secured Mobile Apps.

Questions?

Please contact Texas National Bank – Customer service at **(855) 862-1920** or email **customerservice@texasnational.com** regarding questions about the information included in this Mobile Privacy Disclosure or questions about our Mobile Apps.

For a complete list of how we collect and share your personal information you can also access the bank's Privacy Policy found at **[Texas National Bank Privacy Policy].**

MOBILE PRIVACY DISCLOSURE

Rev. 02/2022

Definitions	
Geo-Location Information	Geolocation is the identification of the geographic location of a device, such as a mobile phone, gadget, laptop, and server. By using the geolocation of the IP address of the mobile device the physical location of the device can be identified. The geolocation of your mobile device when you first signed up for online banking services is collected and used to identify and authenticate your device and you as an authorized user when you return to use the online service again in the future.
Biometric Face or Fingerprint Recognition / Authentication	Biometric authentication is a security process that relies on the unique biological characteristics of individuals to verify they are who they say they are. Biometric identification uses biometrics, such as Facial, fingerprints or retina scans, to *identify* a person, whereas biometric authentication is the use of biometrics to *verify* people are who they claim to be.
IP Address (Mobile Device ID Information)	IP Address (Internet protocol address) is an identifying number this is associated with a specific computer device or computer network. When connected to the internet, the IP address allows the computers to send and receive data / information. This is used and required to ensure the safe and secured transfer of information and data between your device and the online banking network.
Cookies / Beacons	Cookies / Beacons are small electronic files that web servers typically send to users' computer when they visit a website. Cookies are stored as text files on users' hard drive and can be accessed by web servers when the user visits a website. A session cookie is a cookie that stores information as a user is using the Site but is deleted once the browser session is finished. A persistent cookie is a cookie that stores information as a user utilizes the Site and stores and uses that information in connection with future visits of the user to the Site. This information is general used to enhance the users experience while visiting a Site and improve its performance of the Site by, among other things, allowing the website owners to monitor the Site performance, making the Site easier to use, measuring the effectiveness of promotional placements, and tailoring the Site (including the ads and offers a user receives) to better match a user's interests and preferences. You can block cookies by changing the settings on your internet browser. Please note, however if you choose to block cookies, you may not be able to log onto our secured Mobile Apps, and you may disable or limit other functionalities of the Mobile Apps rendering it unusable.
Third-Party Providers	A Third-Party Provider is an authorized online service and platform provider that has been introduced as functioning on behalf of the financial institution**.** They exist outside of your relationship with your bank but may be involved in the online transactions you carry out. There are two types of Third-Party Provider (TPP), and Payment Initiation Service Provider (PISP). These are often under a contractual agreement for the purpose of servicing or processing of financial products and services on behalf of the financial institution.