» DEPOSIT ACCOUNTS
» LOANS
» OTHER SERVICES

PRIVACY & SECURITY

Privacy | Web Security

FACTS	WHAT DOES FRANKLIN STATE BANK DO WITH YOUR PERSONAL INFORMATION?
Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.
What?	The types of personal information we collect and share depend on the product or service you have with us. This information can include: ■ Social Security number and income ■ account balances and payment history ■ credit history and credit scores When you are *no longer* our customer, we continue to share your information as described in this notice.
How?	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons Franklin State Bank chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does Franklin State Bank share?	Can you limit this sharing?
For our everyday business purposes - Such as to process your transactions, maintain Your account(s), respond to court orders and legal Investigations, or report to credit bureaus	Yes	No
For our marketing purposes - to offer our products and services to you	No	We don't share
For joint marketing with other financial companies	No	We don't share
For our affiliates' everyday business purposes - information about your transactions and experiences	No	We don't share
For our affiliates' everyday business purposes - information about your creditworthiness	No	We don't share
For affiliates to market you	No	We don't share
For nonaffiliates to market you	No	We don't share

Questions	Call 308-425-6225 ~ Franklin State Bank

Who we are	
Who is providing this notice?	Franklin State Bank

What we do	
How does Franklin State Bank protect my personal information?	To protect your personal information from unauthorized Access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings.
How does Franklin State Bank collect my personal information?	We collect your personal information, for example, when you ■ open an account or deposit money ■ pay your bills or apply for a loan ■ use your credit or debit card We also collect your personal information from others, such as credit bureaus, affiliates, or other companies.
Why can't I limit all sharing?	Federal law gives you the right to limit only ■ sharing for affiliates' everyday business purposesâ€"information about your creditworthiness ■ affiliates from using your information to market to you ■ sharing for nonaffiliates to market to you

Definitions	
Affiliates	Companies related by common ownership or control. They can be financial and non-financial companies. ▪ *Franklin State Bank does not share with our affiliates*
Nonaffiliates	Companies not related by common ownership or control. They can be financial and non-financial companies. ▪ *Franklin State Bank does not share with non affiliates so they can market to you.*
Joint Marketing	A formal agreement between nonaffiliated financial companies that together market financial products or services to you. ▪ *Franklin State Bank does not jointly market.*

back to top

WEB SECURITY

Online Security

- **Never click on suspicious links** in emails, tweets, posts, nor online advertising. Links can take you to a different website than their labels indicate. Typing an address in your browser instead of clicking a link in an email is a safer alternative.
- **Only give sensitive information to websites using encryption** so your information is protected as it travels across the Internet. Verify the web address begins with "https://" (the "s" is for secure) rather than just "http://". Some browsers also display a closed padlock.
- **Do not trust sites with certificate warnings or errors.** These messages could be caused by your connection being intercepted or the web server misrepresenting its identity.
- **Avoid using public computers or public wireless access points** for online banking and other activities involving sensitive information when possible.
- **Always "sign out" or "log off"** of password protected websites when finished to prevent unauthorized access. Simply closing the browser window may not actually end your session.
- **Be cautious of unsolicited phone calls, emails, or texts** directing you to a website or requesting information.

General PC Security

- **Maintain active and up-to-date antivirus protection** provided by a reputable vendor. Schedule regular scans of your computer in addition to real-time scanning.
- **Update your software frequently** to ensure you have the latest security patches. This includes your computer's operating system and other installed software (e.g. Web Browsers, Adobe Flash Player, Adobe Reader, Java, Microsoft Office, etc.).
- **Automate software updates**, when the software supports it, to ensure it's not overlooked.
- **If you suspect your computer is infected with malware**, discontinue using it for banking, shopping, or other activities involving sensitive information. Use security software and/or professional help to find and remove malware.
- **Use firewalls** on your local network to add another layer of protection for all the devices that connect through the firewall (e.g. PCs, smart phones, and tablets).
- **Require a password to gain access.** Log off or lock your computer when not in use.
- **Use a cable lock to physically secure laptops**, when the device is stored in an untrusted location.

Passwords

- **Create a unique password for all the different systems you use.** If you don't then one breach leaves all your accounts vulnerable.
- **Never share your password over the phone, in texts, by email, or in person.** If you are asked for your password it's probably a scam.
- **Use unpredictable passwords** with a combination of lowercase letters, capital letters, numbers, and special characters.
- **The longer the password, the tougher it is to crack.** Use a password with at least 8 characters. Every additional character exponentially strengthens a password.
- **Avoid using obvious passwords** such as:
  - your name
  - your business name
  - family member names
  - your user name
  - birthdates
  - dictionary words
- **Choose a password you can remember without writing it down.** If you do choose to write it down, store it in a secure location.

Website Spoofing

Website spoofing is the act of creating a fake website to mislead individuals into sharing sensitive information. Spoof websites are typically made to look exactly like a legitimate website published by a trusted organization.

Prevention Tips:

- Pay attention to the web address (URL) of websites. A website may look legitimate, but the URL may have a variation in spelling or use a different domain.
- If you are suspicious of a website, close it and contact the company directly.
- Do not click links on social networking sites, pop-up windows, or non-trusted websites. Links can take you to a different website than their labels indicate. Typing an address in your browser is a safer alternative.

- Only give sensitive information to websites using a secure connection. Verify the web address begins with "https://" (the "s" is for secure) rather than just "http://".
- Avoid using websites when your browser displays certificate errors or warnings.

Caller ID Spoofing

Believe it or not, the number appearing on your caller id box may not be the true telephone number that the call is coming from. For a small fee, criminals can purchase technology that will allow them to display any phone number they want on ***your caller id!***

This is how it works.

- A Spoofer would call an unsuspecting victim and have a local police department, court house, or some other municipal phone number appears on the victim's caller id. The Spoofer would go on to explain to the victim, that there is a problem and the victim has not reported to jury duty. The Spoofer would then go on to tell the victim, â€œWell, maybe I have the wrong person. Why don't you tell me your social security number and we can get this straightened outâ€. The victim, convinced they are speaking with a trusted authority, is then tricked into giving their personal identification information to the Spoofer.
- The scenario that the Spoofer uses may change, but the premise stays the same, they are attempting to scare you into giving them personal information. If you are ever contacted on the phone by someone asking for personal information, the best thing to do is hang up and call them back to verify they are who they say they are and that the phone number is accurate.

Phishing

Phishing is when an attacker attempts to acquire information by masquerading as a trustworthy entity in an electronic communication. Phishing messages often direct the recipient to a spoof website. Phishing attacks are typically carried out through email, instant messaging, telephone calls, and text messages (SMS).

Prevention Tips:

- Delete email and text messages that ask you to confirm or provide sensitive information. Legitimate companies don't ask for sensitive information through email or text messages.
- Beware of visiting website addresses sent to you in an unsolicited message.
- Even if you feel the message is legitimate, type web addresses into your browser or use bookmarks instead of clicking links contained in messages.
- Try to independently verify any details given in the message directly with the company.
- Utilize anti-phishing features available in your email client and/or web browser.
- Utilize an email SPAM filtering solution to help prevent phishing emails from being delivered.

Report Fraudulent or Suspicious Activity

- Report any suspected fraud to your bank and the fraud units of the three credit reporting agencies immediately.
- TransUnion: (800) 680-7289
Experian: (888) 397-3742
Equifax: (888) 766-0008

If you become a victim, contact:

- The fraud departments of the three major credit reporting agencies
- The creditors of any accounts that have been misused
- The local police to file a report
- The bank to cancel existing accounts held in your name and re-open new accounts with new passwords

We are committed to safeguarding our customers' financial information. Maintaining our customers' trust and confidence is a top priority. To learn more about how we protect your information, you may view our Privacy Statement by accessing it from the home page of our website.

Identity Theft

What is Identity Theft?
Identity theft occurs when someone acquires your personal information and uses it without your knowledge to commit fraud or theft. It is a serious crime and cases are growing. An all-too-common example is when an identity thief uses your personal information to open a credit card account in your name.

No matter how cautious you are, there is no way to completely prevent identity theft from occurring. But there are ways you can help minimize your risk. This page contains valuable information on how you can protect yourself by managing your personal information wisely, the warning signs of identity theft, and what to do if you do become a victim.

Helpful Tips

Don't give out personal information on the phone, through the mail or over the Internet unless you've initiated the contact or are sure you know whom you're dealing with.

- Don't carry your Social Security card with you; leave it in a secure place. Carry only the identification and credit and debit cards that you need.
- Don't put your address, phone number, or driver's license number on credit card sales receipts.
- Social Security numbers or phone numbers should not be put on your checks.
- Shred your charge receipts, copies of credit applications, insurance forms, physician statements, checks and bank statements, expired charge cards that you're discarding, and credit offers you get in the mail.
- Secure your credit card, bank, and phone accounts with passwords. Avoid using easily available information like birth date, the last four digits of your SSN, or your phone number. When opening new accounts, you may find that many businesses still have a line on their applications for your mother's maiden name. Use a password instead.
- Secure personal information in your home, particularly if you have roommates or hire outside help.
- Promptly remove mail from your mailbox. If you're planning to be away from home and can't pick up your mail, call the U.S. Postal Service to request a vacation hold.
- Ask about information security procedures in your workplace. Find out who has access to your personal information and verify that records are kept in a secure location. Ask about the disposal procedures for those records as well.
- Before revealing any personally identifying information (for example, on an application), find out how it will be used and secured, and whether it will be shared with others. Ask if you have a choice about the use of your information. Can you choose to have it kept confidential?

Check your credit report
Order copies of your credit report once a year to ensure accuracy. You may call 1-877-322-8228 for a FREE credit report from any or all three credit reporting agencies. (The law allows credit bureaus to charge for additional copies of your credit report).

Make sure it is accurate and includes only those activities you have authorized.

By checking your report on a regular basis you can catch mistakes and fraud before they wreak havoc on your personal finances. Don't underestimate the importance of this step.

Credit Bureaus
Log on to www.annualcreditreport.com to get your credit report from all three credit reporting agencies -- Experian, Equifax and TransUnion -- once every 12 months for free.

Equifax - www.equifax.com. To order your report, call: 1-877-322-8228
Experian - www.experian.com or call 1-888-EXPERIAN (397-3742)
TransUnion - www.transunion.com. To order your report, call: 800-888-4213. To report fraud, call: 1-800-680-7289

back to top