

## **Citizens State Bank Debit Card Application**

	Name (Please Print):	
	2 <sup>nd</sup> Emboss Line:	
Primary Checking Account Number:		**This account will be debited for purchases.
☐ <b>Maintenance</b> (Same Card Number) <b>***Verify customer address and phone number***</b>		
Last 4	digits of Card Number:	
<ul> <li>Reorder Card</li> <li>Change Name (don't forget to change CIF)</li> <li>Add Account(s)</li> </ul>		<ul> <li>PIN Reset</li> <li>Change CIF (CIF #)</li> <li>Remove Account(s)</li> </ul>
	Account(s) Added or Removed: Checking	Savings
□ New Card Issuance (New Card Number) Last 4 digits of Card Number:		
Last 4		
	CIF Number:	
	Address:	
City / State / Zip Code:		
	Phone Number:	
	Additional Accounts: Checking	Savings
	have received a copy of the Citizens State Bank Debit Card Agreement and agree o the terms outlined in the agreement and authorize the issuance of a debit card. elect to "opt out" of VISA Account Updater (VAU); I understand by "opting out" participating Reoccurring Payment Merchants will NOT automatically receive my new card information for reoccurring payments.	
SIGNATURE	:	_DATE:

## Citizens State Bank Debit Card Customer Agreement

- 1. Your agreement relating to your deposit, loan and other accounts will govern your use of this card.
- 2. Use of the debit card is subject to the terms and provisions of the Texas Business and Commerce Code, the Texas Banking Code, the Electronic Funds Transfer Act, and any present and future legally enacted codes, statutes, regulations, and laws.
- 3. The debit card is a service to our customers and all card privileges can be cancelled at any time. If we do so, you are required to return the card when asked.
- 4. The PIN chosen by you is for your security purposes. The numbers are confidential and should not be disclosed to third parties or recorded on the card. You are responsible for safekeeping your PIN(s). You agree not to disclose or otherwise make your PIN available to anyone not authorized to sign on your accounts.
- 5. Tell us, at once, if you believe your VISA debit card has been lost or stolen or of any unauthorized transactions. Your liability for unauthorized VISA point of sale transactions that take place on the VISA system is Zero dollars (\$0.00). We may require you to provide a written statement regarding claims of unauthorized VISA debit card transactions. These provisions limiting your liability do not apply to VISA commercial credit cards, ATM transactions, or PIN transactions not processed by VISA; and apply only to cards issued in the United States. With respect to unauthorized transactions, these limits may be exceeded to the extent allowed under applicable law if we determine that you were grossly negligent or fraudulent in the handling of your account or debit card.
- 6. To the extent permitted by law, Citizens State Bank reserves the right to change the transaction limits without notice and may also require the use of your PIN to complete transactions at certain merchants to maintain or restore security.
- 7. You may make cash withdrawals up to a maximum of **\$600** and purchase up to **\$3000** worth of goods and services per day (if there are sufficient funds in your account).
- 8. Only the primary checking account will be debited for purchases.
- 9. After 24 consecutive months of inactivity, your debit card will be closed. A new debit card or replacement debit card not activated within 6 months of the issuance date will be closed.
- 10. VISA requires all financial institutions to participate in VISA Account Updater (VAU). This service will allow <u>participating</u> merchants to receive your updated card information when you receive a new card from us. To avoid late payments and penalties, you must check with your merchant to ensure your card information is updated. All cardholders are automatically enrolled in VISA Account Updater—there's nothing you need to do to initiate this service. You must notify the bank if you choose not to participate in VISA Account Updater (VAU) for each card issued by Citizens State Bank. To "opt out" visit your local CSB location or call us at 979-596-1421.
- 11. As issuers of Automated Teller Machine (ATM) access devices, we have provided for your information a list of safety precautions regarding the use of automated teller machines. Please read the following safety precautions:
  - When using walk-up or drive-up unmanned automated teller machines (ATMs) -
  - Remain aware of surroundings, particularly at night, and exercise caution when withdrawing funds;
  - Inspect an ATM before use for possible tampering, or for the presence of an unauthorized attachment that could capture information from the access device or your Personal Identification Number (PIN);
  - Refrain from displaying cash and put it away as soon as the transaction is completed; and
  - Wait to count cash until you are in the safety of a locked enclosure, such as your car or home.
  - Do not reveal your personal identification number (PIN) to others. Avoid allowing others to view your PIN entry into an ATM. Memorize your PIN and do not write your personal identification number or code on your ATM access device.
  - Safeguard and protect your access device. Treat it as if it were cash, and if it has an embedded chip, keep the device in a safety envelope to avoid undetected and unauthorized scanning.
  - Promptly report a lost or stolen access device and report all crimes to law enforcement officials immediately.
  - If you observe suspicious persons or circumstances while approaching or using an ATM, do not use the machine or, if you are in the middle of a transaction, cancel the transaction, take the access device, leave the area, and come back another time or use an ATM at another location.
  - Safeguard and securely dispose of ATM receipts.
  - Do not surrender information about your access device over the telephone or over the Internet, unless to a trusted merchant in a call or transaction initiated by you.
  - Promptly review your monthly statement and compare ATM receipts against your statement to protect against ATM fraud.
  - If purchasing online with the access device, end transactions by logging out of websites rather than simply closing the web browser to protect against Internet fraud.