GOLDEN STATE BANK

PLEASE READ THE ENTIRE AGREEMENT CAREFULLY BEFORE ENROLLING IN THE SERVICE OR INITIATING ANY TRANSACTIONS.

ELECTRONIC BANKING AGREEMENT AND DISCLOSURE

This Agreement and Disclosure sets forth your and our rights and responsibilities concerning the use of our Electronic Banking Product. In this agreement, the words “you” and “your” mean those who sign as applicants or any authorized user(s). The words “we”, “us” and “our” mean the Bank. By using our Electronic Banking product, you agree to all of the terms and conditions of this Agreement. Our E-Banking website is found at www.goldenstatebank.com.

ELECTRONIC BANKING FEATURES: You may access your account information by using a specific E-Banking User ID and PIN assigned to you. At the present time you may use the system to:

General Electronic Banking

- Perform inquiries on checking, savings, certificate accounts, and loans.
- Obtain statement transaction detail on your accounts.
- Transfer funds between your Golden State Bank deposit accounts.
- Initiate instructions for placing a stop payment on your checking account.
- Submit a check re-order request.
- Send e-mail messages to the Bank.

Bill Payment

- Initiate bill payments to any merchant or vendor you choose in the United States.

Cash Management Features (Commercial customers only; additional agreements required)

FEES AND CHARGES:

- There is no monthly fee for General Electronic Banking features.
- Standard Bank fees will be assessed for completed wire transfers and stop payments.
- Standard check fees will be assessed when check orders are processed.
- There is no monthly fee to add Bill Payment features.
- Cash Management features will become available to commercial customers as part of their General Electronic Banking features.

USER ID AND PIN: The User ID and PIN issued to you is for your security purposes. Your PIN is confidential and should not be disclosed to third parties. You are responsible for safekeeping your PIN. You may change your PIN and User ID at any time by clicking on “management” under Home Banking. For security purposes, the system will automatically prompt you to change your PIN if you have not changed it in 90 days. You should carefully select a PIN that is hard to guess. (We suggest

that you stay away from names, dates, and information that may be easily guessed.) Your PIN must be 6 to 8 characters long and must include letters and numbers. You agree not to disclose or otherwise make your PIN available to anyone not authorized to sign on your accounts.

In order to ensure the security of our records, we will end your online session if we have detected no activity for 10 minutes. This is to protect you in case you accidentally leave your computer unattended while you are logged on. When you return to your computer, simply sign on again to continue your session. If you are processing several bill payments during an E-Banking session, we suggest that you periodically submit those payments in order to keep your E-Banking session active.

NO SIGNATURE REQUIREMENT: When any payment or other on-line service generates items to be charged to your account, you agree that we may debit the designated account without requiring your signature on the item and without any notice to you.

NOTICE OF LIABILITY: Tell us AT ONCE if you believe your PIN has been lost or stolen. Telephoning is the best way of keeping your possible losses down. You could lose all the money in your account (plus your maximum overdraft line of credit.) If you tell us within two (2) business days, you can lose no more than $50.00 if someone used your PIN without your permission. If you do NOT tell us within two (2) business days after you learn of the loss, and we can prove that we could have stopped someone from using your PIN without your permission if you had told us, you could lose as much as $500.00.

If our statement shows transactions that you did not make, tell us at once. If you do not tell us within sixty (60) days after the statement was mailed to you, you may not get back any money lost after the sixty (60) days if we can prove that we could have stopped someone from taking the money if you had told us in time. If a good reason (such as a long trip or hospital stay) kept you from telling us, we may extend the time period. If you believe that your PIN has been lost or stolen or that someone has transferred or may transfer money from your account without your permission, call or email the Bank.

BUSINESS DAYS: Our business days are Monday through Friday. Holidays are not included.

CUTOFF TIMES: The following cutoff times pertain to specific Electronic Banking Features. Transactions received after the cutoff time will be processed the following business day.

- Funds Transfers – 5:00 p.m. PST.
- Wire Transfers – Domestic – 1:30pmp.m. PST (noon), International – 11:00 a.m. PST.
- Bill Payments – 11:00 a.m. PST. To ensure that your payment is properly credited to your account prior to the payment due date; please allow at least five (5) business days from the date payment is submitted for your payment to reach your merchant or vendor.
- Stop Payments – 5:00 p.m. PST.

DOCUMENTATION: Periodic Statement: You will receive a monthly account statement from us on your checking account(s). For savings accounts, you will receive either a monthly or quarterly statement depending on whether you have electronic activity on your account. Your account statements must be reviewed in a timely manner after receipt for any unauthorized activity represented.

Confirmation or Receipt: A confirmation or receipt will be displayed at the time you make a transfer, submit a bill payment, initiate cash management transactions, or submit instructions for wire transfers, stop payments or check orders. This confirmation or receipt should be printed and kept for your records.

OUR LIABILITY FOR INCOMPLETE TRANSACTIONS: If we do not complete a transaction to or from your account on time or in the correct amount according to our agreement with you, we will be liable for your losses or damages only to the extent of the amount of your payment or transfer that should have occurred if we are unable to resolve the problem, and only to the extent the law allows. However, there are some exceptions. We will NOT be liable for instance:

- If, through no fault of ours, you do not have enough money in your account to cover the transaction.
- If the money in your account is subject to legal process or other claim restricting such transaction.
- If the transaction would go over the credit limit on your overdraft line.
- If the terminal or system was not working properly and you knew about the breakdown when you started the transaction.
- If circumstances beyond our control (such as fire or flood) prevent the transaction, despite reasonable precautions that we have taken.
- If any information provided by you about the payee on a bill payment is incorrect.
- If there are any delays in handling the payment by the payee.

ELECTRONIC BANKING RELATIONSHIP: If you are a business customer, you certify that the business applying for Electronic Banking has conducted the appropriate meeting and completed the appropriate documentation indicating that the business is authorized to enter into an electronic banking relationship. This documentation will be made available to the Bank upon request.

STOP PAYMENTS: Stop Payment requests made before 5:00 PM PST, Monday through Friday, will be effective that same day. Stop Payment requests made after 5:00 PM PST, Monday through Friday, on a weekend or a holiday, may not be effective until the following business day. Your account will be charged the Bank's standard fee for placing a stop payment at which time the Stop Payment request will be valid for 6 months from the date the Stop Payment request was originally made through E-Banking.

Stop Payment Rights: If you have told us in advance to make regular electronic fund transfers or

preauthorized transfers out of your account(s), you can stop any of these payments. Here is how: You can send a Stop Payment request to the Bank through E-Banking, or you can call us or write to us at the telephone number or address set forth in this agreement, in time for us to receive your request three (3) business days or more before the payment is scheduled to be made. We may also require you to put your request in writing and get it to us within fourteen (14) days after you call. We will charge you the standard charge for each stop payment request you give. Liability for Failure to Stop Payment of Preauthorized Transfers. If you order us to stop one of these payments three (3) business days or more before the transfer is scheduled, and you have provided us with accurate information, and we do not stop payment, we will be liable for your losses or damages.

IN CASE OF ERRORS OR QUESTIONS: Call us at 909-981-8000 or write the Bank at P. O. Box 430, Upland, CA 91785 or at info@goldenstatebank.com if you think your statement or receipt is wrong or if you need more information about a transaction listed on the statement or receipt. We must hear from you no later than sixty (60) days after we sent the first statement on which the problem or error appeared.

When you contact us, be sure to provide us with the following information:

- Tell us your name and account number.
- Describe the error or the transfer you are unsure about and explain as clearly as you can why you believe it is an error or why you need more information.
- Tell us the dollar amount of the suspected error.
- Confirmation or Receipt number.
- For Bill Payment errors tell us.
    - Checking account number used to pay the bill.
    - Payee name.
    - Date the payment was sent.
    - Payment amount.
    - Payee account number.

We will tell you the results of our investigation within ten (10) business days after we hear from you and will correct any error promptly. If we need more time, however, we may take up to forty-five (45) calendar days to investigate your complaint or questions. If a notice or error involves an electronic funds transfer that was initiated in a foreign location, the applicable time period for action shall be twenty (20) business days in place of ten (10) business days, and ninety (90) calendar days in place of forty five (45) calendar days.

If we decide we need more time, we will recredit your account within ten (10) business days for the amount you think is in error, so that you have the use of the money during the time it takes us to complete our investigation. If we ask you to put your complaint in writing and we do not receive it within ten (10) business days, we may not recredit your account.

If we decide that there was no error, we will reverse the recredit made to your account (if applicable) and send you a written explanation of our findings within three (3) business days after we finish our investigation. You may ask for copies of the documents that we used in our investigation.

CONFIDENTIALITY: We will disclose information to third parties about your account or the transactions you make:

- To complete transactions as necessary;
- To verify the existence and condition of your account upon the request of a third party, such as a credit bureau or merchant; or
- To comply with government agency or court orders; or
- If you give us your written permission.

VIRUS PROTECTION: The Bank is not responsible for any electronic virus or viruses that you may encounter. We encourage our customers to routinely scan their PC and diskettes using a reliable virus software product to detect and remove any viruses. Undetected or un-repaired viruses may corrupt and destroy your programs, files and even your hardware. Additionally, you may unintentionally transmit the virus to other computers.

NOTICES: All notices from us will be effective when we have mailed them or delivered them to your last known address on our records. Notices from you will be effective when received by us at the telephone number or the address specified in this agreement. We reserve the right to change the terms and conditions upon which this service is offered. We will mail notice to you at least thirty (30) days before the effective date of any change, as required by law. Use of this service is subject to existing regulations governing the Bank and your account(s) and any future changes to those regulations.

ENFORCEMENT: In the event either party brings a legal action to enforce this agreement or collects amounts owing as a result of any account transaction, the prevailing party shall be entitled to reasonable attorneys' fees and costs, including fees on any appeal, subject to any limits under applicable law.

TERMINATION: You agree that we may terminate this agreement if:

- You, or any authorized user of your PIN, breach this or any other agreement with us;
- We have reason to believe that there has been an unauthorized use of your account or PIN;
- We notify you or any other party to your account that we have cancelled or will cancel this Agreement.
- You or any other party to your account can terminate this Agreement by notifying us in writing.

Termination of service will be effective the first business day following receipt of your written notice. Termination of this Agreement will not affect the rights and responsibilities of the parties under this Agreement for transactions initiated before termination.

E-BANKING SYSTEM (EBS) SECURITY

A number of advanced security features are incorporated within the E-Banking System (EBS). The EBS system provides convenient banking anytime, anywhere without compromising your security or privacy.

The security features we employ protect your information throughout your E-Banking (also referred to as Electronic Banking) session.

The following security features are utilized:

- **User ID and PINs:** Only your valid User ID and PIN will allow you to log on.
- **Automatic Log-Off:** If no action is taken for 10 minutes, your internet banking session will be automatically terminated, and you will be logged off.
- **Access disabled after a set number of incorrect attempts:** To protect against someone attempting to guess your PIN, your User ID is disabled after 3 incorrect attempts. You must then contact the Bank to reactivate your User ID.
- **128-bit SSL encryption:** Your information is encrypted and scrambled as it is sent across the Internet. SSL uses public key cryptography to secure transmissions over the Internet so only the EBS server and your browser are able to interpret the information. SSL also uses authentication via a digital ID to ensure you are communicating with the Bank. This prevents another computer from impersonating the Bank. Finally, SSL detects if data integrity has been compromised during transmission and closes the connection if any tampering occurred.
- **Expiring PINs:** Your PIN will expire every 90 days. You are required to change your PIN every 90 days.
- **Ongoing security reviews and technology upgrades:** We constantly evaluate the latest security techniques and upgrade our systems as security improvements are developed.
- **Continuous monitoring for potential problems:** Our systems are monitored for potential problems that could compromise system security or privacy.

Protecting Your Information

PINs are a critical component of EBS security. **Your PIN MUST be kept confidential**. You should memorize your PIN and should not write it down. You are responsible for keeping your PIN, account numbers and account information confidential.

If you lose or forget your PIN, contact the Bank to have your default PIN enabled. You will be required to change your PIN the first time you log on to maintain your secure access. If you think someone has stolen your PIN or is trying to access your account information to transfer money without permission, notify the Bank immediately. You should also log on and change your current PIN as soon as possible.

Never give your PIN out over the phone, even to a Bank employee. **A BANK EMPLOYEE WILL NEVER NEED TO KNOW YOUR PIN AND YOU SHOULD NEVER GIVE IT TO SOMEONE CLAIMING TO BE A BANK EMPLOYEE.** To ensure that the EBS security measures work, it is extremely important for you to choose PINs that are difficult to guess. PINs must NOT be related to one's job or personal life. For example, a car license plate number, a spouse's name, or parts of an address should not be used.

Choose easily remembered PINs that are at the same time difficult for unauthorized parties by:

- stringing several words together (the resulting PINs are also known as "pass phrases").
- shifting a word up, down, left or right one row on the keyboard.
- bumping characters in a word a certain number of letters up or down the alphabet.
- transforming a regular word according to a specific method, such as making every other letter a number reflecting its position in the word.
- deliberately misspelling a word (but not a common misspelling).
- combining a number of personal facts like birth dates and favorite colors.

To make guessing more difficult, PINs must be six to eight characters long. To ensure that a compromised PIN is not misused on a long-term basis, PINs must be changed every 90 days.

Finally, never walk away from your computer with account information displayed. Instead Exit and close your browser when you have completed your session.

We have taken every reasonable precaution to ensure your privacy and account security; however, we are not liable for security breaches beyond our control.

To print this page please refer to the Disclosures page
https://www.goldenstatebank.com/disclosures