Security Statement

With online banking, and as with traditional banking methods, security is a prime concern for Pacific Western Bank. Our online banking platform brings forth a combination of industry-standard security technologies to protect both customer and Bank data from exposure to unauthorized entities. This level of security is achieved in part by:

- Protecting the privacy and the confidentiality of the communications between your browser and our servers.
- Verifying that only authorized persons are allowed to access online banking.
- Maintaining isolation of our computers from the internet.

Security and User Identification

Online security is achieved by credential verification. To begin an online session, a user must have a User ID and a Password. Commercial customer users must also have a Company ID. Customers accept responsibility for the confidentiality and security of access credentials. For security purposes, passwords must be changed during the initial log-in to our online banking platform and then every ninety (90) days. Customers determine passwords based on Bank-defined conventions. Customers play a crucial role in preventing others from logging on to their account(s). Customers should never use passwords that are easy to guess. Examples of bad passwords include birth dates, first names, pet names, addresses, phone numbers, social security numbers, etc. Customers should never reveal passwords to another person. You may register your device when accessing online banking through use of a Secure Access Code delivered to mobile devices or landlines for commercial customers and delivered via email, mobile devices, or landlines for retail customers; this assists the Bank in authenticating access.

Commercial customers are granted customized access based on services. The Bank will provide access credentials to an authorized Company Administrator. Company Administrators have full account access and are responsible for maintaining users, which includes adding, assigning entitlements and removal of users. In addition, we may provide company users additional layered security methods due to Cash Management services granted. Customers agree that the security credentials assigned by the Bank constitute a reasonable security procedure, and the Bank can rely on, and act in accordance with, any inquiry, message or instruction transmitted electronically using the assigned security credentials, which will constitute conclusive evidence that such inquiry, message or instruction is correct and has been duly authorized by the company.

Lockouts

Our system also uses a lock-out protocol to deter unauthorized users from repeated login attempts. After a certain number of unsuccessful login attempts, the system locks the user out, requiring a phone call to the Bank to verify the identity of the customer or successful login using an approved User ID and Password after a period of time, before re-entry to a secured session.

Online Banking Security

Customers are encouraged to take advantage of additional online banking tools offered which add another layer of protection, under the “Security” and “Alerts” tab of the user profile. As a precaution, specific account alerts are automatically sent for invalid password attempts and password changes.

Secure Data Transfer

Communication between the customer and Admin User browsers and the online banking web servers is performed over the Internet and employs TLS1.2 encryption. The TLS certificates employ 3DES_EDE_CBC with SHA2 for message authentication and RSA for key exchange. Online banking also performs various layers of validation to guard against any tampering during communication.

Validation layers include cross-site scripting, cross-site request forgery, and business layer validation to ensure relationships

A firewall between the Internet and the DMZ (demilitarized zone) allows only legitimate web traffic through. Intrusion Detection (IDS) and Intrusion Prevention (IPS) systems deployed at various locations are also part of a comprehensive network security implementation.

Protecting your User ID and Password

You should not keep your User ID and password information on or near your computer. Keep both in a secure area away from your computer to prevent any unauthorized access to your accounts. Never share your User ID or password with anyone. For security reasons, we auto enforce password changes every ninety (90) days. Some browser software may store user names and passwords to make it easier when you revisit a website. Pacific Western Bank does not recommend using this feature to access sites containing sensitive information. You can disable this feature in your browser. Please note that if you enable this feature, unauthorized users may be able to access your account without your knowledge. Do not leave your computer while you are logged into online banking, especially if others may have access to your computer. Before leaving your computer, be sure to click on the Log Off option or EXIT button to end your online session.

Secure Email

You understand you may send and receive secure email messages to and from the Bank through online banking. Messages sent to the Bank through online banking will automatically be routed to a Bank email box. The Bank is not responsible for any delay in messages being retrieved. Urgent messages should be verified by a telephone call to the Bank. You are responsible for periodically checking for messages sent by the Bank. You cannot use secure email to stop payments, transfer funds or perform bill payment.

Regular non-encrypted internet email may not be secure and should not be used as a method to communicate sensitive information. If you are uncertain about the security of an email or the confidentiality of any message, you can contact our Electronic Banking Department by phone at 1.800.350.3557, by mail at Pacific Western Bank – Electronic Banking, PO Box 131207, Carlsbad, CA 92013-1207, or by visiting your branch of account. Please use the Find A Location feature on our website home page for information on our branch offices.

Best Practices to Mitigate Phishing Scams

An increasingly prevalent scam currently being employed by unscrupulous individuals is phishing. Phishing is a high-tech scam that uses unsolicited email (also known as spam) or pop-up messages in an attempt to deceive you into disclosing your credit card numbers, bank account information, social security number, passwords, and/or other sensitive information. Spoofing is one person or program pretending to be something it's not on the internet, usually via an email or website.

The sophistication of phishing and spoofing scams sent out to consumers continues to dramatically increase. While online banking is widely considered to be as safe as or safer than in-branch or ATM banking, as a general rule, you should be careful about giving out your personal financial information over the internet. Remember, Pacific Western Bank will never request your personal information via email or text.

Recommendations to follow to avoid becoming a victim of scams:

- Be suspicious of any email with urgent requests for personal financial information. Phishers have been known to include upsetting or enticing (but false) statements in their emails to get people to react immediately. More recently, some phishers have toned down their language, as email

recipients have become more aware of the use of this tactic. Either way, the email typically asks for information such as login IDs, passwords, credit card numbers, social security numbers, etc.

- Be careful of emails that not are personalized and/or may contain spelling errors and/or awkward syntax and phrasing. Many phishing emails are sent in bulk and, therefore, are not personalized. If you are suspicious of an email claiming to be from a company you do business with, call the company which appears to have sent the email before responding. Many emails are being sent from other countries from individuals for whom English is a foreign language, thus resulting in misspelled words and awkward syntax and phrasing.
- Be careful of personalized emails that ask for personal financial information. Be suspicious of any email that contains some personal financial information, such as a whole or partial bank account number and asks for other information, such as a PIN. We will never ask for or send you personal financial information by email unless it is encrypted or by some other secure method.
- Do not use links in an email to get to any web page. Instead, call the company on the telephone to confirm the web page address, or log onto the website directly by typing in the web address in your browser.
- Do not complete forms in email messages that ask for personal financial information. Pacific Western Bank would never ask you to complete such a form within an email message. Only communicate information, such as credit cards numbers or account information, via a secure website or the telephone. When submitting financial information to a website, look for the padlock or key icon, and make sure the internet address begins with "https:". A secure web server designation can be found by checking the beginning of the web address in your browser's bar and the address should begin with https:// rather than http://.
- Regularly log on to your online accounts and check your bank, credit and debit card statements to ensure that all transactions are legitimate. One of the real advantages of banking online is being able to review your account for unauthorized or unusual activity. If anything is suspicious, contact your bank and all card issuers immediately.
- Ensure that your browser is up to date and security patches are applied. Always visit your browser's home page to download the latest security updates even if they don't alert you to do so.
- Use online statements to reduce the volume of paper mailed. Today, paper is the cause of more actual instances of identity fraud than are electronic thefts.

Disclaimer

Pacific Western Bank does not intend to offer investment advice nor act as a fiduciary by publishing any information contained in this site or at linked sites. Third-party information made available on or through this website is provided "as-is," without warranty of any kind, either expressed or implied, including (without limitation) any warranty of accuracy, completeness or adequacy of the information, title, non-infringement of third-party rights, merchantability, or fitness for a particular purpose.

Except as otherwise required by law or set forth in our agreements with users, we assume no responsibility for any damages, expenses or losses, including without limitation, direct or indirect, special, incidental or consequential damages arising in connection with this website use thereof or reliance on any information contained herein, even if we are unaware of the possibility of such damages.

Protecting Children's Privacy Online

From our websites, we do not knowingly collect or use personal information from children under thirteen (13) without obtaining verifiable consent from their parents. However, we are not responsible for data collection and use practices from nonaffiliated third parties to which our website may link.

For more information about the Children's Online Privacy Protection Act (COPPA), please visit the FTC website at www.ftc.gov.

Changes to this Statement

We may add to, delete from, or otherwise change the terms of this Statement from time to time. We may notify you of the changes by mail, email, or by posting a modified Statement on our website. Your continued use of this site or any online service following such notification will constitute your acceptance of the revised Statement. Accordingly, please check this site regularly for revisions.

Questions

If you have any questions regarding this Statement, you can write to us at Pacific Western Bank – Electronic Banking, PO Box 131207, Carlsbad, CA 92013-1207 or call us at 1.800.350.3557.