



Stockmen's Online Security Statement

Introduction

The Stockmen's Bank ("Bank") brings together a combination of industry approved security technologies to protect data for the Bank and for you, our customer. It features User and Password -controlled system entry, a VeriSign- issued Digital ID for the bank's server, Secured Sockets Layer (SSL) protocol for data encryption, and a router loaded with a firewall to regulate the inflow and outflow of server traffic. Although we have taken the necessary steps to put in place a security infrastructure, you as the Online Banking user also play an important role in protecting your accounts.

Secure Access and Verification Process

Upon enrollment for Stockmen's Online, the Bank will assign you a Stockmen's Online user name (Stockmen's Online ID) and a temporary password. During your first time login, you'll be prompted to change the temporary password. See below for additional password information. You should make your password hard to guess (avoid names, significant dates, or other information easily guessed). You are responsible for safekeeping your Password and User Name. You may change your Password and User Name at any time by clicking on "options" during your Online Banking session. For security purposes and your protection, the Bank recommends that you change your password every 90 days. You agree not to disclose or otherwise make your Password or User Name available to anyone not authorized to sign on your account.

In order to ensure the security of your 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 onto the Stockmen's Online. Should this occur, simply sign on again to continue your session.

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 Personal Computers and diskettes using a reliable software product to detect and remove any viruses. Undetected or unrepaired viruses may corrupt, destroy your program files, data, or compromise your passwords. Additionally, you may unintentionally transmit the virus to other computers.

Minimum System Requirements

An internet capable machine:
Microsoft Internet Explorer 5.0 or higher
Netscape Navigator 7.0 or higher
Browser Cookies enabled

Protecting Your Information

Your Password:

It must be at least six to eight characters in length. (Longer is generally better.)
It must contain at least one alphabetic and one numeric character.
It should not be information easily obtainable about you. This includes license plate, social security, telephone numbers, or street address.

<http://www.stockmensbank.com>

Password Expiration:

All passwords for newly activated User Names must be changed at first use. This way only the person assigned the User Name knows the password.

Protecting your Passwords:

To ensure security, passwords must be used carefully. These recommendations will help protect your passwords:

Never write down your password.

Never share your Password with anyone.

Never use your Stockmen's Online logon password for another purpose.

Change your password immediately if you think it has been compromised.

You should use care to not save your Password on your computer. Some dialog boxes, such as those for remote access and other telephone connections, present an option to save or remember your password. Do not select that option.

The Stockmen's Bank will never ask you for your password, you should never give this information out to anyone, even to a trusted source.

A Bank Employee will never need to know your Password and you should never give it to someone claiming to be a Bank Employee.

Security Tips

Keep your operating system up to date. If your computer is more than five years old, the operating system (e.g. Windows 95, 98, etc.) may not offer the same level of protection as newer systems. System manufacturers provide frequent updates to help make your system more secure.

Use a current Web browser. To provide our customers with the most secure online access to their accounts, Stockmen's Online systems requires a minimum of:

An Internet Capable Machine:

Internet Explorer 5.0 or higher
Netscape Navigator 7.0 or higher
and browser cookies must be enabled.

New browsers, especially security updates to these browsers sometimes are available on a monthly basis. It is recommended that you visit your software manufactures website at:

www.microsoft.com/security

<http://info.apple.com>

Install a personal firewall. Check to see if your operating system already includes a firewall prior to purchasing a separate one. There are many firewalls available including:

Sygate Personal Firewall

http://smb.sygate.com/download_buy.htm

McAfee Personal firewall:

<http://us.mcafee.com>

ZoneAlarm Personal Firewall

<http://www.zonelabs.com>

Install and update anti-virus software. Virus protection software helps reduce the risk of contracting computer viruses that can compromise your security. These programs offer continuous upgrades in response to the latest threats. Some of the most popular programs are:

<http://us.mcafee.com>

<http://www.norton.com>

Activate a pop-up blocker. Several free, publicly available programs exist that will block all pop-up windows from occurring while you are online. Perform an Internet search for "pop-up blocker" or look at the options provided by major search engines. Here are some of the leading companies:

<http://toolbar.google.com/>
<http://toolbar.msn.com/>
<http://toolbar.yahoo.com/>

If you have activated the pop-up blocker, please be aware the system "time out" warning message will also be blocked and the final screen will remain visible on your monitor.

Scan your computer for spyware regularly. You can eliminate potentially risky pop-up windows by removing any spyware or adware installed on your computer. Spyware and adware are programs that look in on your Web viewing activity and potentially relay information to a disreputable source. Perform an Internet search for "spyware" or "adware" to find free spyware removal programs. You should confirm that these programs are from legitimate companies before downloading. As with a pop-up blocker, you will want to be sure that your removal program is not blocking, or removing, wanted items, and if it is, consider turning it off on some Web sites.

Use secure Web sites for transactions and shopping. Be sure the Web page you are viewing offers encryption of your data. Often you will see a lock symbol in the lower right-hand corner of your browser window, or the Web address of the page you are viewing will begin with "https://". The "s" indicates "secured" and means the Web page uses encryption. The Stockmen's Bank, for instance, provides 128-bit encryption – the highest level commercially available today.

Avoid downloading programs from unknown sources. Downloads from unfamiliar sources may contain hidden programs or viruses that can compromise your computer's security.

Your Liability

Notify us AT ONCE if you believe your Password or User Name has been compromised, lost, or stolen. Telephone us immediately at 1-(866) 350-1407 between 7:00 a.m. Mountain Standard Time and 6:00 p.m. Mountain Standard Time or the next business day (Monday through Friday). If you notify us within two (2) business days, your maximum liability is no more than \$50.00 if someone used your Password without your permission. If you do NOT notify us within two (2) business days after you learn of the loss, and information is available evidencing that we could have prevented someone from using your Password without your permission if you had notified us, your maximum liability is \$500.00. Without a notification, your liability could be the total balance in your account (plus your maximum overdraft line of credit).

If your statement shows transactions that you did not make, notify us at once. If you do not notify us within sixty (60) days after the statement was mailed, you risk not being refunded any funds lost after the sixty (60) days if information is available evidencing that we could have prevented someone from taking the funds if you had notified us in time. If a valid reason (such as a long trip or hospital stay) kept you from notifying us, we may extend the time period. If you believe that your Password has been lost or stolen or that someone has transferred or may transfer money from your account without your permission, call, write or e-mail the Bank immediately.

Business Days

Every day is a business day except Saturday, Sunday, and Federal Holidays.

Cut off times

The following times are designed as cutoff times pertaining to specific Online Banking Transactions. Transactions received after the cutoff time will be processed the following business day.

<http://www.stockmensbank.com>

Funds Transfers	6:00 p.m Arizona Time
Automated Clearinghouse Entries	1:00 p.m. Arizona Time
Wire Transfers	2:00 p.m. Arizona Time
Stop Payments	6:00 p.m. Arizona Time
Bill Payment	1:00 a.m. & 11:00 p.m. Arizona Time

The Stockmen's Bank Liability

IN NO EVENT WILL THE STOCKMEN'S BANK OR ITS STOCKMEN'S ONLINE THIRD PARTY PROVIDER, BE LIABLE TO THE CUSTOMER FOR ANY DAMAGES, INCLUDING LOST PROFITS, LOST SAVINGS OR OTHER DIRECT, INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM AND DOCUMENTATION, OR FOR ANY CLAIM BY ANOTHER PARTY. THE STOCKMEN'S BANK'S DUTIES AND RESPONSIBILITIES IN CONNECTION WITH ACH AND WIRE TRANSFERS ARE LIMITED TO THOSE DESCRIBED IN THIS AGREEMENT. THE STOCKMEN'S BANK WILL BE DEEMED TO HAVE EXERCISED ORDINARY CARE AND TO HAVE ACTED REASONABLY IF THE STOCKMEN'S BANK HAS ACTED IN ACCORDANCE WITH THE TERMS OF THIS AGREEMENT AND WILL BE LIABLE FOR LOSS SUSTAINED BY CUSTOMER ONLY TO THE EXTENT SUCH LOSS IS CAUSED BY THE STOCKMEN'S BANK'S GROSS NEGLIGENCE OR WILLFUL MISCONDUCT. THE STOCKMEN'S BANK WILL NOT BE LIABLE FOR ANY CONSEQUENTIAL, SPECIAL OR PUNITIVE DAMAGES, REGARDLESS OF THE STOCKMEN'S BANK'S ACT OR OMISSION. THE STOCKMEN'S BANK WILL HAVE NO LIABILITY FOR ANY LOSS OR DAMAGE:

- RELATED TO THE DISHONESTY OF THE CUSTOMER'S EMPLOYEES, OFFICERS OR AGENTS;
- RESULTING FROM ANY RECEIVING FINANCIAL INSTITUTION'S FAILURE TO ACCEPT ANY ACH OR FUNDS TRANSFER REQUESTS;
- RESULTING FROM ANY DELAY IN THE PERFORMANCE OF THIS AGREEMENT, WHICH IS CAUSED BY AN ACT OF GOD, FIRE OR OTHER CASUALTY, ELECTRICAL OR COMPUTER FAILURE, DELAYS OR FAILURE TO ACT BY ANY CARRIER, MEDIUM OR AGENT OPERATING BETWEEN THE STOCKMEN'S BANK AND THE CUSTOMER OR BETWEEN THE STOCKMEN'S BANK AND THIRD PARTIES OR ANY OTHER CONDITION OUTSIDE THE STOCKMEN'S BANK'S CONTROL. NO THIRD PARTY WILL HAVE RIGHTS OR CLAIMS AGAINST THE STOCKMEN'S BANK UNDER THIS AGREEMENT. THE TERMS OF THIS SECTION WILL SURVIVE TERMINATION OF THIS AGREEMENT.

In Case of Errors or Questions

The Stockmen's Bank	or	onlinesupport@stockmensbank.com
Attn.: Online Banking Manager	or	1-(866) 350-1407
3825 Stockton Hill Road		
Kingman, AZ. 86401		