



ARROWHEAD BANK

INTERNET/ELECTRONIC SPECIAL SECURITY SERVICES

Arrowhead Bank has incorporated layered security methods to our electronic security services to strengthen the effectiveness of our fraud prevention efforts. This document will explain some of the services that are associated with our Debit Card and Internet Banking systems. Customers may have a choice on activating some of these security features, but others will be standard. All of our security methods and controls are not disclosed in order to maintain certain additional monitoring and fraud detection techniques remain proprietary and confidential.

Debit Cards

Debit cards are issued to customers to provide a convenient way to pay for goods and services and access cash at ATMs or at merchants. Visa rules establish the primary security framework for these access devices that can use the ATM networks or Visa credit card channels to complete the transaction. If selecting “debit” at the time of purchase, the systems will route the transaction through the ATM network where a PIN is used as the primary security authorization. If “credit” is selected, the transaction is routed through the credit card network and relies on a signature or Visa rules for security requirements and the handling of disputes. It is important to remember that there are a few differences between a debit card from a credit card. The biggest one that many customers are not aware of is that a debit card does not have the right to dispute a charge due to a disagreement with the service or product that was purchased from a merchant. Therefore, if you feel that you may need to retain that right, use a credit card instead of your debit card because the bank will not be able to dispute the charge once it has posted.

These are some of the other security features that are incorporated into debit card transactions.

- **Visa Card & Security Code Requirements:** The Visa system has specific card production requirements that include a magnetic data stripe and a security code on the back-side. Although there have been several large security breaches, counterfeiters still need to obtain this information to be able to create a card that can be swiped at merchants. The security code is often used when the card is used over a telephone and serves as a mini-PIN. Many pay-at-the-pump locations are now also requiring the cardholder’s Zip Code as an identification requirement.
- **Real-Time Host Connection:** Our bank is directly connected to the ATM & Visa networks so we can approve, deny, and mark-up transactions as they are received. This allows you the ability to see inter-day transactions and use the most up-to-date balance for making the pay/deny decision. If you make a deposit during the day, you will be able to make a purchase on your card.
- **Real-Time Fraud Analytics:** We have a very sophisticated software tool that is reviewing all transaction activity to help identify potential fraud threats. Although it is not fool-proof, when we do suspect a problem we will initiate a call to the cardholder and/or suspend the card until we can confirm that it has not been compromised.
- **Optional Vacation Alerts:** Since we look for unusual activity, this includes out-of-territory transactions. So if you are going to travel, contact our staff so we can update the system for that time period and general locations to avoid the automatic suspension of your debit card when the first transaction is attempted.
- **Default Daily Limits:** The bank has established a daily maximum dollar amount that will be approved on a daily basis for both ATM and Point-of-Sale transactions. This security setting reduces the ability to take all your funds in the account during one day. If you feel that you will need to have a higher limit for a short time or specific transaction, contact the bank and we can adjust your setting to meet your needs. We can also lower your limit upon request.. However, we strongly recommend that you do not leave the limit above our standard limits of \$500 for ATMs and \$1,000 for POS transactions.



ARROWHEAD BANK

- **PINs:** When using the “debit” option, a PIN is required. (In some cases, the PIN will not be required if the purchase is under \$25.00.) This PIN can be set to whatever 4 digit code you like, but you will need to contact our customer service department to complete the change on our systems. Do NOT write your code on the card or place it in your wallet. Also, do not share your PIN with others, including family members.
- **Transaction Confirmations (e-Commerce & International in particular):** As part of our daily review process, we will attempt to verify certain transactions that might be suspicious. You may receive an email, text or phone call from our staff just checking to make sure that you did authorize the transaction.
- **Internet Banking Mark-ups:** With our real-time connection, we are able to mark-up your approved transactions on our Internet system to help you keep track of every item as they are approved during the day.
- **Visa Zero Liability:** Under Visa’s rules, there is a zero liability clause that does provide consumers with an additional level of protection where they should not be charged the \$50 maximum liability that is allowed under Regulation E for fraudulent or unauthorized transactions.
- **Optional Transaction Alerts (Text and or Email):** Arrowhead Bank offers a free service that *we highly recommend* for all our debit card users. You can receive a Text or Email alert within minutes for every attempted debit card transaction. This is a great fraud prevention and recordkeeping tool that will help identify potential fraud attempts immediately. To set the Text, Email (or both types) of alerts on your cards, contact any of our Arrowhead Bank representatives.

Internet Banking Services

The services offered over the Internet represent a growing fraud threat due to the ability to transfer funds to other banks using some for the special services, such as External Exchange, ACH Origination and Wire Transfers. This service also poses a potential threat for the theft of confidential financial information since it will contain account information and statements. Therefore, we have incorporated multiple layers of security into the service to provide secondary levels of authentication besides the initial Logon ID and Password. This section will explain some, but not all, of our security tools to help make sure your information and funds are safe and secure.

- **Multi-Channel Enabled:** We have certain features, authentication, authorization and alert features that can be sent via the Internet (email), telephone (voice) and SMS (text) to provide alternative methods to prevent a single point of security compromise. Some of the special services, especially related to funds transfers to external institutions, will receive greater scrutiny. Additional authentication methods that use an out-of-band (not using an internet based account or email) approval may be required or recommended to combat the man-in-the-middle or man-in-the-browser attack.
- **Computer Registration:** Although we never rely only on computer identification as a primary control due to the possibility of compromised security cookies, it does offer a level of security for unsophisticated attacks. The system requires that any PC that attempts to logon to the system that has not been previously registered (has the security cookie on the PC), completes the registration process. The security code is sent to the user’s registered email or phone (text) for entry prior to allowing access. This code will be used to register the PC and create the security cookie. (As noted below, the system can require the code be sent only to a phone (text) to provide an out-of-band registration. Also, the system can be set to require the registration for every logon attempt to eliminate the threat of a compromised cookie.
- **IP Reputation Tools:** When our security experts identify potentially dangerous/fraudulent internet sites (as identified by their IP address), we will update our systems to block any access to or from those sites. This is just one of our extra security efforts we employ continuously to protect our customers from potential threats.
- **Automatic Logoffs (Time-Outs):** After 10 minutes of inactivity, your online banking session automatically ‘times-out’ and will require you to re-enter your password.



ARROWHEAD BANK

- **Mobile Authorization Code:** When using our mobile web-browser application designed to fit on a cell phone screen, you will be required to enter the MAC code. This is similar to the computer registration code. This is a 4 digit code and is required when you request the Mobile access under the “Preferences” drop-down menu.
- **Passwords:** We do require unique passwords for every user. The password must be from 8 to 15 digits and include at least one capital letter, one number and one special character. We can also set your password to automatically expire upon your request as an optional security setting.
- **Enhanced User Rights & Limits:** Our system allows us to set customized rights and limits by users that can restrict activity and features to only what is desired or recommended by the bank. Limits on funds transfer rights and amounts will minimize the risk of unauthorized transactions.
- **External Funds Independent Pre-processing Confirmations:** Prior to completing funds transfers to other institutions for certain transactions, our staff may send out confirmation requests or acknowledgments to make sure the user was aware of the request prior to its completion. A brief delay prior to final processing allows a limited amount of time for you to notify the bank if the transaction was not authorized. If no notice is received, the transaction will be sent unless there are additional security concerns identified by our staff or systems.
- **Risk & Fraud Software Analytics:** Our online banking vendor has incorporated a sophisticated software application that will review user behavior and transaction risks to help identify unusual or suspicious activity to automatically alert you and the bank of a possible need for additional approvals or reviews. Although this is not fool-proof, it does add yet another layer of risk mitigation against account take-overs.
- **Funds Transfer Back-Office Reviews:** Our staff reviews every transaction as it is prepared for processing and does ongoing reviews for suspicious or unusual activity. When identified, we proactively contact our customers for approval prior to processing the transactions.
- **Optional Administrative New User/Recipient Alerts:** For our Cash Management Administrative users, an alert (email, text or voice) can be automatically sent whenever a new sub-user or recipient is added to the company profile. This alert will let you know that a potential unauthorized user or recipient was entered on our system.
- **Optional One-Time Use Registrations:** If desired, we can require you to register you PC every time you logon to prevent the possibility of your security cookie being compromised.
- **Optional Voice or Text Only Computer Registration:** As mentioned in the Computer Registration explanation, we can require that only out-of-band registration codes be allowed (no emails). This provides protection against the attacks where the user’s PC and email account has been compromised. Contact our customer service department to add this security setting to your Logon ID.
- **Password Expiration:** Your password is currently set to require you to choose a new password every 365 days. You may also change your password at any time using the Security options under the Preferences drop-down menu.
- **Optional Dual-Authorization:** For certain funds transfer transactions (funds transfers, ACH Originations, EFTPS and Wires) we can set your rights to where another user tied to your account must approve the transaction to provide a secondary authorization.
- **Optional Out-of-Band Authorization:** Similar to the Dual-Authorizations, we have another security feature that will require approval from an out-of-band source, like your cell phone. It will send a text alert when a funds transfer has been created and needs a reply from the phone message to complete the transaction.
- **Optional Physical or Soft Tokens:** We have the ability to require a code generated by a secure token (either a physical fob or a mobile app) to be entered for any monetary transaction. The token will automatically generate a new secure code after a short period of time that will be confirmed by our system prior to allowing the transaction to be processed.



ARROWHEAD BANK

- **User Customizable Alerts (Balance & Transaction driven):** Within our Internet Banking system, our vendor has created fully customizable alerts that you can set up to monitor transaction activity, balances and balance changes. You may also choose to be notified by alerts for different types of security processes on your online account, such as successful logins, security changes made, passcode changed and external transfer accounts processed. Use the different Alert options under the Notify Me Alerts tab to set these alerts up. You may also need to set up your primary contact information under the Security option in that same area. There is a HELP link on the screen that will provide more information on how to set up specific alerts if you need assistance.

Mobile Apps and Tablet/iPads Services

Advances in technology continue to make accessing your financial information more convenient. The tablets/iPads can view our Internet Banking system using a browser that will size the information to display better for the smaller sized screen with these devices. We also have a mobile app that is available on iPhones and Android phones. We do allow you to view balances, transaction activity/history, and cleared checks on your checking and savings accounts. You can also perform transfers between your linked accounts and make payments to billers already existing your online banking account.

Things You Can Do To Help

Despite our best efforts to protect our systems and provide layered security, you do have an active role to play in helping prevent fraud. Here is a quick list of some tips to live by:

- Sign up for Alerts (for both debit cards and the Internet services)
- Pick good passwords and change every 90 days
- Request other optional security methods such as dual authorizations and tokens (Commercial Customers only) for your monetary transactions
- Secure your PC, laptop, tablet, iPad and cell phones to require a code/password to be required after a limited amount of time with no activity and guard against theft of these access devices
- Keep virus detection, spyware, malware current
- Activate your personal firewall on your computer
- Keep operating system and browser patches current
- Do not click on links in emails unless you are sure they are from a trusted source
- Don't install a plug-in or program on your computer unless you know it is legitimate
- Do not post personal information on your Internet profiles
- Shred your documents with confidential information before throwing out
- Review your account activity frequently and balance monthly statements
- Log out of your account when you are done
- Don't use any public computer for accessing your accounts
- Activate as many of the optional security tools that seem appropriate for your needs
- Report any unusual activity immediately

We hope you found this information useful in explaining our security protection and optional services that you may want to consider. If you have any suggestions on how we can improve on our services or security protection, please let us know.