



## Individuals and Consumers: What You Need to Know About Electronic Banking

One of Pendleton Community Bank's top priorities is protecting your financial information when you bank and pay bills online. When you apply for an online banking and bill payment account, the bank performs multiple steps to confirm your identity prior to opening the account. After you are assigned an online banking and bill payment account, you are responsible for reviewing and abiding by the terms in the Agreement and Disclosure for 24/7 Online Banking.

Pendleton Community Bank will NEVER ask for your online banking user ID and PIN by phone, email, in person or any other means of communication. DO NOT provide your online banking user ID and/or PIN to any request online, by phone or in person. Providing this information may allow a criminal to compromise deposit accounts used with online banking and bill payment. Immediately contact your nearest Pendleton Community Bank office if you are contacted and asked to provide your online banking log on credentials.

State of the art technology is used to keep your information secure. All passwords and personal information is encrypted and access requires passwords only you know. Your account numbers, social security numbers and/or tax id numbers are never displayed on the online banking system.

Within online banking is a secure email portal. The bank may use this secure email portal to respond to your request for online banking/bill payment assistance and sensitive information can be securely communicated using this online banking email system.

Pendleton Community Bank utilizes multifactor authentication and pictures for your online banking protection. During your online banking setup, you will pick a unique picture that appears on every page in online banking and you are asked to setup three questions and answers. Always verify that your unique picture shows when you log into your online banking account. Certain activities in online banking may require you to provide the answer to the questions you created. If you are unable to correctly answer the questions, your account is locked and you have to contact a Pendleton Community Bank representative. The representative will verify your identity and unlock your online banking account.

You are protected from financial loss if your online banking credentials are used without your permission. The amount of the loss you can incur if your online banking account is compromised depends on how quickly you contact Pendleton Community Bank. Refer to the *Agreement and Disclosure for 24/7 Online Banking, Customer Liabilities – Consumer Customers Only* for losses you may be responsible for.

If you believe your online banking PIN is lost or stolen, or that someone has used or will use your account without your permission, notify Pendleton Community Bank immediately. You are not protected from financial loss if you give your online banking User ID and the PIN to a friend or relative and they take all or a large portion of money from your account. If you have given your User ID and PIN to a friend or relative and suspect they may now misuse it, immediately contact Pendleton Community Bank.

You are protected from financial loss if you are forced to use your online banking user ID and PIN or a thief obtained your online banking user ID and PIN through fraud or robbery. However, you should immediately notify the bank of the theft or robbery.

### **Protect Your Computer**

Below are suggestions on how to keep your computer safe for online banking and bill payment.

- (1) Install anti-virus and anti-spyware software. Keep the software up-to-date and run regular security scans.
- (2) Learn how to use your computer's personal firewall.
- (3) Install the latest updates and/or patches for your web browser (Internet Explorer, Firefox, etc.).
- (4) Disable the option in your browser that remembers your username and password, thus allowing automatic log on.
- (5) Disable file sharing software so unauthorized users cannot access your computer and its data.

### **Online Banking Best Practices**

Safe online banking relies on you making good choices and following a few simple online banking guidelines.

- (1) Your password should consist of numbers and letters, should be at least 8 characters in length and should be changed at least every 60 days. If you have to write your password down, keep it in a safe location. [Click here](#) to view tips for creating a strong password and tips for keeping your password secure.
- (2) Never leave your computer unattended once you have logged into your online banking account and ensure no one is watching when you enter your online banking ID and PIN.
- (3) Sign out of your online banking account, clear your web browser cache and close your web browser when you have completed your online banking transactions.
- (4) Do not give your bank account number, online banking password or user ID to anyone requesting it, regardless if the request comes via an email or telephone call. Pendleton Community Bank will never call or email you requesting this information. [Click here](#) to view FDIC information on 'Phishing', identity theft and how to protect yourself or [Click here](#) to view the US-CERT (United States Computer Emergency Readiness Team) website for information on Phishing and how to protect yourself.
- (5) Avoid performing online banking transactions on a public computer. If you must use a public computer, change your password after completing your transactions.
- (6) Never save your bank account number or other sensitive information on a publically accessed computer.
- (7) Know who you are dealing with. Access your online banking account by typing the bank's address in your web browser. Never go to a website from a link in an email and then enter your user ID or PIN. Report any unusual account activity immediately to Pendleton Community Bank.
- (8) Go to [Tips for Safe Banking Over the Internet](#) published by The Federal Deposit Insurance Corporation (FDIC).

### **Pendleton Community Bank Contact Information**

Franklin Office – (304) 358-2311  
Marlinton Office – (304) 799-6700  
Moorefield Office – (304) 538-7900

Petersburg Office – (304) 257-4000  
Harrisonburg Office – (540) 434-4722

Email: [mail@yourbank.com](mailto:mail@yourbank.com) (this is not a secure email so please do not include personal information like account numbers, SSN, etc.)