



Mobile Banking & Mobile Remote Deposit Capture Best Practices

Below are some great habits to form when using our remote services. For questions concerning your account, please feel free to contact us at 301.627.2666 or 800.952.7428.

1. Utilize security features for your personal mobile devices such as passcodes to gain entry.
2. Disable the device from the Mobile Banking application through your online banking account if you suspect it has been stolen.
3. Avoid using unsecured, public Wi-Fi networks to access financial accounts with mobile devices – Always use your cellular network when conducting mobile financial services
4. Only download apps from stores, such as Apple & Android.
5. Know that PGFCU will not ask users to provide confidential information over an email or SMS message – any communication in such form is *NOT* from Prince George's Community Federal Credit Union.
6. We recommend you retain the original scanned items for a minimum of 30 days after deposit. Items should be kept under lock and key and destroyed after 30 days.
7. The Mobile Remote Deposit Capture program retains electronic images of your deposited items. Be sure to safeguard your device, Username and Password to prevent unauthorized access to this information.
8. In the event of application failure, please notify PGCFUC immediately. While many failures can be remedied remotely, in the event that you cannot scan a deposit, we will make every effort to get your deposit to Prince George's Community Federal Credit Union on the same business day; however, we cannot guarantee our ability to do so.
9. Remember that you are the first line of defence against fraud. Pay close attention to the checks you deposit. Double check for accuracy in the payee, amount, and signature lines. Be on the lookout for any inconsistencies in the check that could signal alterations or counterfeit items.
10. Members are encouraged to install anti-virus software on their home PC and Android devices.