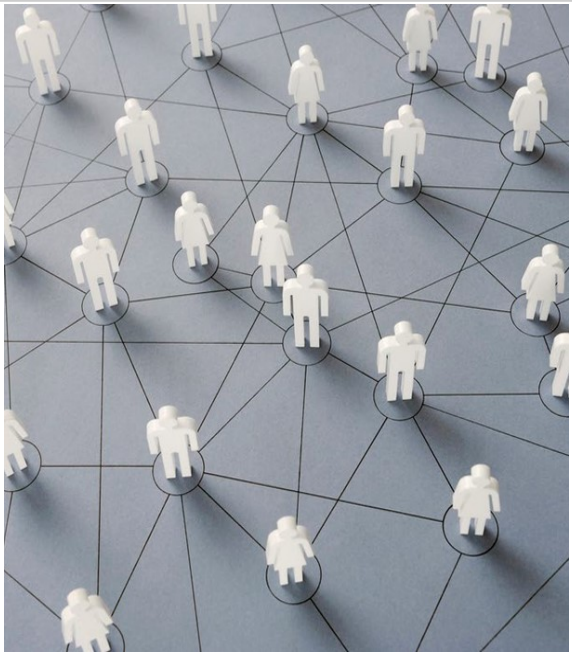
Bank of Botetourt

February 2021 Issue 2

Member FDIC

EQUAL HOUSING LENDER

Mobile Deposit and Remote Deposit Capture–Convenient, But Beware of the Risk



Advances in online banking technology have allowed businesses and average citizens to streamline their banking activities. For those opting to forgo in-person visits to a bank, they can now do almost all transactions via the internet. One of the popular features of online banking is Mobile Deposit Capture (MDC) for consumers. For businesses using this function, it is called Remote Deposit Capture (RDC).

Despite all the bells and whistles of online banking, not all things have been replaced with a click of a button. In the 2019 Federal Reserve Payments Study, it was reported that check payments declined 7.2 percent per year between 2015 to 2018. Even with the decline, it is definitely not something that will be completely eliminated in the near future, and in fact, banking professionals have sought to make manual check writing easier with mobile deposit technology. According to the 2018 Mercator Advisory Group, 25% of consumers use a camera on their smartphone to deposit checks. In this era of a pandemic that is forcing us all to try to remain apart, that number has increased exponentially.

Mobile Deposit Capture (MDC) is a service offered by financial institutions that allows users to scan checks and transmit those scanned images to a bank for posting and clearing by using technology built into the financial institution's apps. Essentially, deposits are made from anywhere without sending paper checks to a financial institution. The basic requirements for an MDC service include a PC or mobile device and an internet connection. MDC has been shown to decrease processing costs and improve customers' accessibility to make deposits since it can literally be done at any time.

Remote Deposit Capture (RDC) also allows for the depositing of checks via the internet. This setup usually includes a PC, a specific scanner (recommended by the financial institution) and a banking application.

Continue on Page 2

Bonsack

Buchanan

Care Center

Cave Spring

Daleville

Eagle Rock

Fairfield

LakeWatch

Lexington

Natural Bridge

Peters Creek

Salem

Troutville

www.bankofbotetourt.com
www.facebook.com/botetourt
(540) 591-5000

Mobile deposits provide substantial benefits to both financial institutions and consumers, but with all technology, there are some risks, the biggest being fraud. Over the years, there has been an increase of bad actors depositing fraudulent checks or purposely depositing one check more than once. Below are some other risks to be mindful of:

- ***Fake Apps***-Scammers can create fake apps that look just like a financial institutions app. Once you enter your personal information the cybercriminal can steal login credentials giving them access to your real bank account. It is always important to verify that you are downloading the legitimate bank app.

- ***Don't use your bank app on a public Wi-Fi***- Public Wi-Fi is a gateway for hackers to access your phone and track what you are doing. It is always better to use a private Wi-Fi network to log into your bank account, but if you need to access your account in public, always use your cellular data.

- ***Don't make your password too easy***- The good news is banking apps no longer allow simplistic passwords and require a mixture of symbols, letters and numbers. That being said, it is important to make sure your banking password is complex and unique to help deter hackers from gaining access to your bank account. Longer passwords or phrases are always harder to hack then shorter passwords.

- ***Update your mobile device operating system or apps***- App developers are constantly improving the look and security of apps. These updates are extremely important because they address vulnerabilities and gaps. Outdated software makes it easier for hackers to break through and exploit vulnerabilities. Whenever your phone notifies you about an update, install it as soon as possible, especially if it is for your mobile banking app.

- ***If the image of your check is blurry or of a poor quality, the image may be rejected*** - It is important to check your account and pay attention to notifications that may alert you to a problem. If you ignore an alert and the check image is not accepted, your funds may not be deposited.

Remote Deposit Capture for businesses also poses some unique risks. In addition to maintaining up-to-date patches on computers used for RDC, additional risks include:

⇒ **Proper training of personnel is a must. If the business does not handle large amounts of checks, less sophisticated systems might be appropriate. Written procedures that are monitored and enforced are one way to mitigate risks.**

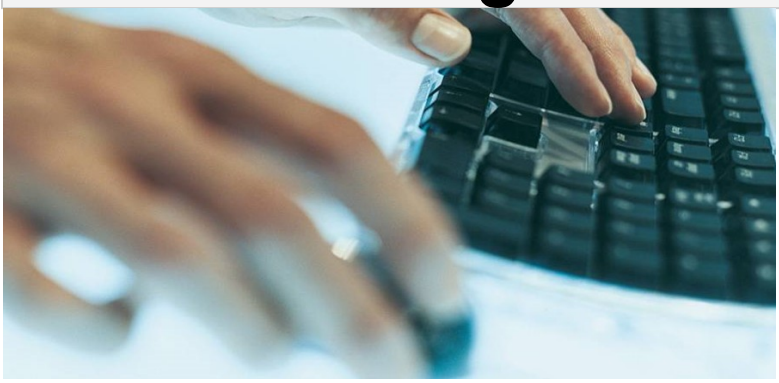
⇒ **Regular inspection and maintenance of scanners is critical to ensure proper functionality.**

⇒ **Best practices would include limiting usage of the RDC computer to only that function. Not allowing employees to use the device to check email can curtail phishing dangers. Segregating the desktop from the rest of the network can also harden security.**

⇒ **A risk assessment of the RDC environment can help identify specific areas of concern that can be mitigated before they blossom into full attacks.**

Sources:
Federal Reserve Board - Federal Reserve Payments Study (FRPS)
https://www.federalreserve.gov/paymentsystems/fr-payments-study.htm
https://www.cutimes.com/2017/06/09/as-Mobile-deposit-capture-soars-so-do-risks/#:~:text=However%2C%20with%20the%20growing%20use,error%20or%20intentionally%20by%20fraudster
https://www.fool.com/the-ascent/banks/articles/7-security-risks-mobile-banking-how-avoid-them/

Seniors Targeted in Online Schemes



Cybercrimes targeting seniors have become extremely prevalent over the past several years. Since 2014 cybercrimes against seniors has cost this demographic over 650 million dollars in losses according to an FBI study on protecting senior citizens from cyberattacks. These types of crimes can be devastating to many older adults and can leave them in a very vulnerable position with little time to recoup their financial losses. The theory has been that seniors are prime targets because they are wealthy. However, it is not just wealthy seniors that are targeted. Many low income and fixed income seniors also have been victims.

Due to the pandemic, seniors have been forced to become more tech-savvy to be able to stay in touch with family and to just get the basic necessities like prescriptions and groceries. Although many may prefer actual computers, a good number of seniors have also embraced their mobile devices, as well. The challenge is helping seniors embrace this new digital era while simultaneously staying safe. Being able to browse the internet is the easy part, but what worries many cybersecurity professionals is the nuances like updating software, having antivirus protection and being able to identify scams such as phishing. The Department of Homeland Security sited that seniors are defrauded at twice the rate of the rest of the population and are also less likely to report the crime for multiple reasons, including they just simply don't know how.

Here are some common schemes that target seniors:

- ***Medicare/Medicaid and Social Security Scams***- Criminals pretend to be government officials in hopes of getting their personal information, or they will provide bogus services for elderly people at fake mobile clinics, then use the personal information they provide to bill Medicare and steal the money.

- ***Telemarketing Scam***s- One of the most common schemes is when scammers use fake telemarketing calls to prey on older people, who are more likely to make twice as many purchases over the phone than the national average.

- ***Counterfeit prescription drugs***-Con artists will use the internet to advertise prescription drugs at lower prices than most pharmacies. Because many seniors are on fixed incomes, they are always looking for the best financial deals. However, this scheme is extremely dangerous because not only are they paying money to a criminal, they also may purchase unsafe substances that can inflict even more harm.

- ***Phishing Emails***-Everyone is susceptible to getting phishing emails, but it may be more difficult for seniors to decipher between what is a legitimate email, especially now. Cybercriminals have been getting better with duplicating websites that sometimes not even the trained eye can tell are not legitimate.

Here are some ways to protect against these types of scams:

⇒ **Always be extremely cautious of unsolicited phone calls.**

⇒ **Be careful what you download. Never open an email attachment from someone you don't know and be wary of email attachments forwarded to you.**

⇒ **Never give or send any personal information, money, checks, or wire information to unverified people or businesses.**

⇒ **Don't give in to the pressure tactics. Scammers create a sense of urgency to create fear which will cause a victim to act quickly. Call the police immediately if you feel there is a danger to yourself or someone you know.**

⇒ **Make sure all computers and mobile devices have an anti-virus and security software. Also make sure to keep them up to date.**

Following the above steps are just a few ways to help protect against senior cybercrimes. There are also a variety of resources that can help you learn to recognize, avoid, and report these types of scams. If you or someone you know has been a victim of a cybercrime it is imperative for it to be reported to the authorities. Reach out to your local police or local FBI unit to file a formal complaint.

Sources:
https://www.cnbc.com/2019/11/23/new-research-pinpoints-how-elderly-people-are-targeted-in-online-scams.html
https://www.ncoa.org/economic-security/money-management/scams-security/top-10-