Federal Deposit Insurance Corporation

feedback

FDIC Consumer News - Winter 2018

A Closer Look at Mobile Banking: More Uses, More Users

What's new, how you can benefit, and how to protect yourself from security risks

With advances in technology, financial institutions are now increasingly providing customers the ability to use mobile phones for banking transactions and to pay for just about anything from a retail purchase to a restaurant bill you're splitting with friends. "Mobile phones provide opportunities for consumers to conduct their banking transactions and make payments from anywhere at any time," said FDIC Senior Technology Specialist Deborah Shaw. "This is a convenient and beneficial way for consumers to incorporate banking and shopping into their busy lives."

Additionally, FDIC research reported in 2016 showed great potential for mobile financial services to help "underserved" consumers obtain more control over their funds and better manage their bank accounts. The FDIC defines underserved consumers as either "unbanked" (they do not have an account at a federally insured financial institution) or "underbanked" (they have an account at a banking institution but they also obtain financial products and services outside of the banking system, such as check-cashing services). The study, "Opportunities for Mobile Financial Services to Engage Underserved Consumers," is on the FDIC website.

Consumer concerns about safety and security, however, continue to be cited in Federal Reserve Board (Fed) annual reports on mobile financial services (most recently from 2016) as reasons some people do not sign up. Here is the latest overview from ***FDIC Consumer News*** to help consumers better understand the current state of mobile financial services, how they might benefit, and how they can protect themselves against security risks.

Mobile Banking

While many people access their bank accounts by going to their bank, using the telephone or an ATM, or accessing services online with their personal computer, consumers are increasingly using their mobile banking options. That might involve text messaging the bank, accessing a bank's website, or using mobile applications (apps) to check account balances, retrieve account information or initiate financial transactions.

The Fed survey found that 43 percent of all mobile phone users with bank accounts had used mobile banking in the previous 12 months, up from 22 percent in the agency's 2011 survey. Among mobile banking users with smartphones (cell phones with internet connectivity), 53 percent with bank accounts used mobile banking in the previous 12 months.

"A mobile banking application makes it easy to transfer funds within your bank, perhaps to send money to a child's account there or to confirm if you have enough funds to make a purchase or pay a bill," added Ben Navarro, a policy analyst at the FDIC. "The mobile banking app can also often be used for payments across banks."

Mobile banking also can assist consumers in making informed decisions. According to the Fed survey, 62 percent of mobile banking users checked their account balance on their phone before making a large purchase in the store, and 50 percent decided not to purchase an item as a result of their account balance or credit limit.

As previously reported in the Summer 2016 ***FDIC Consumer News***, consumers also can conveniently deposit checks from practically anywhere by transmitting an electronic image of each check and relevant information.

Many consumers also are using high-tech wristwatches (called "smartwatches") to read bank alerts or to make purchases applied to their credit, debit or prepaid cards (the latter have money deposited on them but they are not linked to a checking or savings account). Ask your bank what services might be available.

At the FDIC, we've been exploring the potential for mobile banking and mobile payments to bring more low- and moderate-income Americans into the financial mainstream. Recent FDIC surveys have shown that more than one in four households are either unbanked or underbanked.

Additional research by the FDIC showed that one-third of underbanked households used mobile banking in the previous 12 months, and one in eight used it as their primary banking method. The findings suggest that the unbanked and underbanked consumers are attracted to the convenience of mobile technology and the improved sense of control it provides.

Mobile Payments

For years, consumers have been using smartphones to make purchases at retailers' sales terminals and person-to-person or "P2P" payment services (mobile apps) to conduct everyday payment transactions among family or friends without exchanging cash or a check.

"One of the benefits of mobile P2P apps is that payments are typically initiated on a mobile device using the recipient's smartphone number or email address," Shaw noted. "In this way, a consumer does not have to give the recipient a bank account or card number in order to make a payment; this information remains behind the scenes."

What's changing recently is that there are increasingly more P2P mobile apps being offered by banks and nonbanks that provide consumers many choices. These apps are going beyond personal payments and including broader options for paying for goods and services at stores and other businesses. In 2017, banks began to offer a new service that enables U.S. mobile banking consumers to send funds from one bank account to another in minutes, using only a recipient's email address or mobile number on a mobile banking app. Some of these services offer recipients quicker access to their received (deposited) funds, typically within minutes during business days.

Security Tips

Here are some suggestions to help consumers be safe and secure as they use mobile banking and payment products and services:

Be proactive in how you protect the data on your mobile devices. Start by using "strong" passwords and PINs. If you're given the option to use more than your username and password to access your bank account or mobile apps on your phone – for example, if you can choose to receive a one-time passcode by email or text message that also will be needed to access a certain account or app – that will provide added security.

Avoid using an unsecured Wi-Fi network, often found in public places, such as coffee shops, because fraudsters might be able to access the information you are transmitting or viewing. Log out of your bank account or mobile app when it's not in use. Just like with your laptop, use a mobile security/anti-virus software and keep it updated.

Take additional precautions in case your device is misplaced, lost or stolen. Set the screen on your mobile phone to lock after a certain amount of time and use a PIN or password and/or a biometric indicator (for example, a fingerprint or facial recognition) to unlock your mobile phone. Likewise, use PINs or other security features enabled on your smartwatch, such as one that will lock the watch if it is not on your wrist or too far from your mobile phone. Don't store your PINs or passwords on your mobile phone or tape it to the underside of your smartwatch or mobile phone.

Consider signing up for transaction alerts from your credit card, bank and mobile app provider. These messages canhelp you identify unauthorized activity quickly. Alternatively, check your transactions regularly on your cards, bank account and mobile app website.

Research any mobile app before downloading and using it. "Make sure you are comfortable that the mobile app is from a reputable source," said Shaw. "Going to the bank's or company's website to find directions for downloading their app can help to ensure you are downloading a legitimate app."

Transaction alerts from your credit card, bank and mobile app provider … can help you identify unauthorized activity quickly.

Be on guard against fraudulent emails or text messages. These communications typically appear to be from a government agency or a legitimate business in order to trick you into divulging valuable personal information (including your birthday, Social Security number, passwords and PIN numbers) that can be used to commit identity theft. The emails and texts could also ask you to click on a link that will install malicious software on your mobile phone and enable the fraudster to gain access to your mobile banking apps.

"To protect yourself, never provide passwords, credit or debit card information, Social Security numbers and similar personal information in response to an unsolicited text message or email," said Michael Benardo, manager of the FDIC's Cyber Fraud and Financial Crimes Section. "If you have any questions regarding the legitimacy of an email or a text, call your bank or mobile app provider, or the business or government agency that claims to have sent the email or text, and be sure to use a phone number you have looked up on your own and not what is in the email or text in question."

Note: These messages are often called "phishing" emails and "smishing" text messages. Phishing is a term given to fraudulent emails "fishing" for valuable personal information, and "smishing" is a variation of that when referring to "Short Message Service" or "SMS" text messages. "Security experts for years have warned consumers about smishing scams, but as more people have smartphones, smishing is becoming more common," Benardo said.

Final Thoughts

When it comes to getting the most from mobile financial services, here's a simple strategy:

1. Review your bank's website to better understand the mobile products and services offered.
2. Read the bank's consumer disclosures to understand what assistance and other options may be available when using the institution's mobile technology.
3. Contact your bank directly with any questions or concerns, especially before you sign up for a new mobile banking or payment service.

Table of Contents Next Story