Mobile and Online Banking - Things to Know

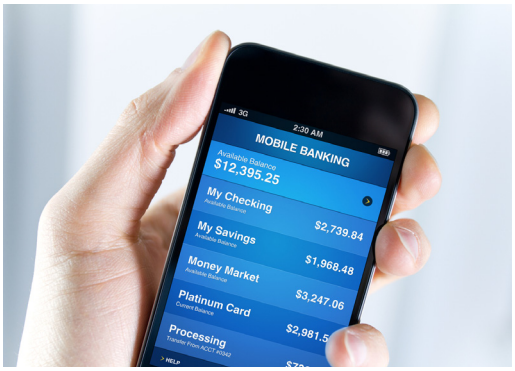
by Sue C. Quimby, CPCU, AU, CIC, CPIW, DAE

Today's on demand society has led to more and more services being offered electronically. One of these services is banking. Deposits can be made, payments submitted or money transferred at the touch of a button, rather than going to the bank and waiting in line. While mobile and online banking can be very convenient, there are some drawbacks, including system outages and most notably fraud. Helping your clients, including financial institutions, understand the potential drawbacks to mobile banking and ways to reduce the exposure is another value-added service of the professional insurance agent.

Electronic financial transactions are not new. Direct deposit has been available in some form since the 1970s. Many people pay their bills online. The advent of mobile technology, especially mobile phones and laptops, greatly increased access to mobile transactions. With mobile banking, deposits can be made simply by taking a picture of the front and back of the check and submitting to the financial institution via the app on the mobile device.

Purchases via mobile devices are convenient and secure. Money is transferred directly to a friend's bank account via P2P (people-to-people or peer-to-peer) applications, eliminating the need for cash when splitting the check for dinner. Wallet apps enable purchases by merely holding the device near the terminal. The seller never sees the actual credit card, and payment information is encrypted.

Mobile banking is extremely popular. A 2018 CITI Mobile Banking Survey of 2000 Americans found that mobile banking apps were the third most popular of all apps. 31% of respondents said they use mobile banking apps most often, following those who use social media apps most often (55%) and weather apps (33%). The survey revealed that approximately half of Americans (46%),



as well as nearly all millennials (86%) have increased their use of mobile banking apps in the past year (www.prnewswire.com). Respondents indicate that they realize time savings averaging 45 minutes per month by using mobile banking apps.

Deposits in financial institutions are usually protected from unlawful withdrawal by Federal Deposit Insurance Corporation (FDIC). However it is up to the individual or business to monitor their statements and notify the bank promptly of any fraudulent transactions, as well as follow security procedures recommended by the bank. Failure to do so can leave the individual or business without recourse for the lost funds, as well as the bank's legal fees. Cyber-crime coverage is one way to protect an individual or business from online banking fraud.

24/7 access is perceived to be the norm. The inability to connect – to check balances, pay bills or other transactions – can be traumatic. However, outages and down times are sometimes unavoidable. For routine system maintenance, financial institutions can reduce their customers' stress by providing advance notice of scheduled down times. Providing alternatives, such as the location and hours of local bank branches, can also increase customer satisfaction.

Potential fraud issues with mobile and online banking include double dipping and smishing. With mobile deposit, the paper check remains with the recipient. Double dipping occurs when the check recipient deposits the check electronically and then attempts to cash it again elsewhere. Insurance companies and agents are examples of entities that can be targets of mobile banking fraud. Checks that have been deposited electronically for claims payments or policy refunds have been returned for reissuance.

Smishing is a form of phishing that is directed at mobile banking customers. A text message claims to be from a bank representative about a purported security problem. The customer is directed to call a toll free number and provide account numbers and PINs. Once the information is provided, the criminals have access to the customer's account. Anyone who receives a suspicious communication, whether by text, e-mail or phone, should contact the customer service phone number on their monthly statement.

There are additional ways to increase mobile and online banking security, such as multiple authentication systems where a text message or code must be entered when logging in. Public unsecured Wi-Fi should be avoided. Set your device so that the screen locks automatically after a certain time. Sign up to receive alerts for transactions, such as purchases above a certain amount. Check accounts regularly to discover any fraudulent activity.

Technology can greatly streamline transactions. However, electronic access can also increase the susceptibility to fraud. Helping clients understand the risks of mobile and online banking and ways to help reduce them is another sign of the true insurance professional.

Previously published in the Insurance Advocate®