Fighting Back Against Mobile Banking Fraud

mobile banking digital banking fraud protection

Summary: Mobile banking has surged. As that trend continues, cyber criminals stand ready to strike. We give you tips to fight back.

Newton's third law states that for every action there is an equal and opposite reaction. So, it should come as no surprise that as mobile banking usage has soared since the onset of the COVID-19 pandemic, so too has mobile banking fraud.

According to a report from the Federal Bureau of Investigation, mobile banking activity increased by 50% in the first five months of 2020. Add to that the stimulus checks that were mailed out to people as part of the CARES Act, and a large portion which were deposited remotely. These are all facts not lost on cyber criminals, who have more incentives to step up their game when it comes to mobile banking fraud. In observance of Cybersecurity Awareness Month , we bring you important information to keep you and your customers safe.

Remote check deposit fraud is on the rise. During the few months that stimulus checks were sent out to recipients to help with the impact of the coronavirus, deposit fraud detection software provider Advanced Fraud Solutions processed roughly 1MM Treasury items for financial institutions, 41K of which were fraudulent. Meanwhile, even before the arrival of the coronavirus, the American Bankers Association estimated that check fraud accounted for 35% of fraud losses within the banking industry. This number could very well rise with the surge in mobile banking and remote check deposits.

ID theft is big. One of the biggest ways that scammers are taking advantage of the uptick in mobile app usage is through identity theft. Using various phishing efforts, scammers are increasingly taking over people's identities to access existing bank accounts or to set up fraudulent accounts that they can then access through a banking app. According to industry experts at Javelin Strategy & Research, fraudsters' efforts are succeeding because some financial institutions are not taking a holistic approach to digital security but are focusing their cybersecurity efforts too much on individual transactions.

Ways to fight back. To keep these predators from causing damage, you should remember to:

1. **Look holistically at your digital security.** Make sure you don't focus only on individual transactions that tend to be siloed between credit cards and debit cards. Review all accounts that are tied together to see if there are any anomalies. New accounts should be especially scrutinized, of course. Use multi-factor authentication for account sign-ins, if possible.
2. **Pay close attention to any sudden contact information changes,** such as email or address changes. Although these updates are generally flagged by bank systems, it can sometimes be too late. Set up your controls to provide you with real-time updates on any changes.
3. **Consider AI applications.** Make sure you don't just send high-risk transactions through a fraud system. Send all data, if possible, through artificial intelligence-based (AI), real-time fraud systems to identify irregularities in customer behavior or suspicious activities.

OUTSOURCE ALM SERVICES AND REST EASY

Regulators have raised the bar on interest rate risk and liquidity analysis, yet there is more to do than there are hours in a day. To see how easy it can be & get expert help, contact us today.