Keeping Your Money Safe: Mobile Account Takeover

Ashlie Hagemann, Fraud Supervisor

Businesses and individuals lose billions of dollars every year due to fraud. While PlainsCapital Bank has a seasoned fraud prevention team in place to protect our customers, we understand that the best protection is education. To that end, our Fraud Prevention Series, "Keeping Your Money Safe," highlights the latest fraud scams with helpful tips on how you can avoid them.

As society becomes more and more mobile dependent, smartphone-related fraud poses a serious threat. From mobile wallets and mobile deposits to online shopping and bill payments, our on-the-go culture of convenience relies on smartphones for just about anything.

This increasing use of smartphones leaves us more vulnerable than ever as fraudsters turn to mobile devices to hijack accounts. Mobile account takeover involves a fraudster using a mobile device to gain access and seize control of an individual's account, resulting in the loss of money or personal information. Mobile account takeovers are on the rise, increasing from 380,000 in 2017 to 679,000 in 2018, according to a Javelin Strategy & Research report.

How Does the Scam Work?

Account takeover has spiked in recent years as fraudsters have found new ways to access bank accounts. Because phone numbers are easier to come by than login credentials, mobile phones are becoming a highly vulnerable target.

One major issue with mobile account takeover is that many customers use their mobile numbers in their account password reset process in order to verify authenticity. After a fraudster hijacks a phone number, they can intercept SMS messages containing authentication codes that can then be used to reset account passwords and take control, locking out the victim. The information they gain provides the fraudster the credentials they need to pose as the user and complete authorization questions, codes, or account updates.

The tricky aspect of mobile account takeover is that scammers are hijacking the victim's phone number, not the physical phone itself. When customers use their mobile device as a way to authenticate their identity, they put themselves at risk of fraud as everything is done digitally, not in-person.

How to Prevent Mobile Account Takeover?

While no single option ensures security, there are approaches that can provide a safer solution. Here are some ways you can protect your information on your mobile device and avoid falling victim to malicious actors:

- **Move away from SMS verifications.** Instead of using SMS texts for authentication codes to verify your account, see if your financial institution offers out-of-band authorization

(OOBA). The process requires two different signals from two different networks or channels, meaning multiple communication channels would need to be compromised for the fraudster to be successful. This form of authentication is typically more sophisticated and a better shield against common forms of hacking and fraud.

- **Institute a 3D Secure 2.0 authentication protocol.** This new standard in authentication aims to reduce fraud and provide added security to online payments. This process allows a cardholder's payment provider to access more data elements around a transaction that can be sent to the cardholder's bank which then assesses the risk level of the transaction and chooses an appropriate action. Data on these transactions can include the shipping address, customer's device ID, previous transaction history, etc.
- **Monitor account activity.** This rule is a given for avoiding any form of identity theft and fraud. The more diligent you are at keeping a close eye on your account activity for anything suspicious, the more likely you are to stop a hacker in their tracks before the fraud gets too far out of hand. In addition, get in the habit of updating your financial institution on any travel plans or upcoming large purchases.

Keeping Your Money Safe

As fraud continues to evolve with the digital age, we must go the extra step to keep our money safe. The best way to avoid mobile account takeover and other scams is to stay vigilant and educate yourself on fraud tactics and prevention methods.

PlainsCapital Bank's Fraud Department provides educational resources for businesses and customers to help detect and prevent fraud on their accounts. For more information about our fraud prevention efforts, visit our fraud resources page.