Protect Against Phone Porting Scams

There is a new method of identity theft growing in threat. Be aware of thieves “porting” mobile numbers out to other providers. When this occurs, crooks can intercept calls and messages while the cell phone becomes inactive. Porting a number to a new provider shuts off usage to the victim’s cell phone and forwards all calls to a new device. Once the thieves gain control of the mobile number, they can request any second factor that is sent to the newly activated device, such as a one-time code sent via text message or an automated call that reads the one-time code aloud.

This new scam works as follows: A fraudster finds out critical information about you such as your name, phone number, Social Security number, date of birth and more. Much of this information is obtainable on the Dark Web. Once the criminal is armed with your information, they call your mobile phone service provider pretending to be you, and tell them that you’re switching to another company but want to keep your current phone number. The transfer of your existing phone number to another carrier is called “porting”. The porting process typically takes up to 24 hours to complete. During this time, both phones will be functional. As a result, any text message that you receive on your phone will also be seen by the scammer on the phone to which your number is being transferred. This leads to further vulnerability. If you have two factor authentication set up on your bank accounts, or any on-line sites for that matter, the scammer will be able to get the code needed to log into your account. From there, you could become a victim of identity theft and risk having money stolen directly from your bank accounts.

Regions Out of Band Authentication requires that you enter a personal Security Code to acknowledge your approval of a transaction. It is important to guard your Security Code and avoid ever making it available to others.

The Better Business Bureau is warning people about scams of this type. Here are some suggestions to protect against porting scams:

• **Inquire with your wireless provider about port-out authorization.** In response to this problem, many providers have implemented security protocols, such as prompting a unique pin or verification question to make porting a phone as difficult as possible.

• **Watch out for “Emergency Calls Only” status.** Call your mobile service provider immediately if you see this status or something similar.

• **Be vigilant about communications you receive.** Watch out for phishing attempts, alert messages or texts in response to two-factor authentication requests.

The cell phone number has become as important as many other personal identifiers. Be on alert to unusual service outages on your device, and report issues to your mobile service provider immediately.